

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

THE TRANSPARENCY PROJECT,

Plaintiffs,

V.

U.S. DEPARTMENT OF JUSTICE,

ET AL.,

Defendants.

Civil Action No. 4:20-cv-467

DECLARATION OF LINDA M. KIYOSAKI

I, LINDA M. KIYOSAKI, hereby declare and state:

1. I am the Chief of Enterprise Guidance Services (“EGS”) at the National Security Agency (“NSA” or “Agency”). I have been in this position since December 2019, and I have been employed with NSA since 1985. I am responsible for oversight of NSA’s Freedom of Information Act Office (“NSA FOIA Office”). This office has primary responsibility for responding to requests for NSA records made pursuant to the Freedom of Information Act (“FOIA”), 5 U.S.C. § 552, and the Privacy Act of 1974 (“PA”), 5 U.S.C. § 552a. I have held a range of significant leadership positions throughout the Agency, and I have a detailed understanding of NSA’s operations, management processes, and resources. Immediately prior to assuming my current position, I was the Deputy Chief of EGS. My other experience includes serving as the Senior Intelligence Analysis Authority; the Associate Director for Strategy, Programs and Performance

for the Mission Management Investment Portfolio; an NSA representative to CIA's Counterterrorism Center; an NSA representative to the FBI; and the Enterprise Engagement and Mission Management Associate Director.

2. I am also a TOP SECRET original classification authority ("OCA") pursuant to Section 1.3 of Executive Order ("E.O.") 13526, dated 29 December 2009 (75 Fed. Reg. 707). It is my responsibility to assert the applicable FOIA/PA exemptions for NSA information in the course of litigation.

3. Through receiving information in my official capacity and in the exercise of my official duties, I have become familiar with the current litigation, which arose out of two FOIA requests filed by The Transparency Project and its Executive Director/Counsel, Ty Clevenger (hereinafter "Plaintiff").

4. The purpose of this declaration is to explain to the Court NSA's origin and mission, explain the role of signals intelligence ("SIGINT") in safeguarding national security, explain the authority to classify national intelligence information, and describe how NSA properly processed the Plaintiff's FOIA requests. Additionally, I will explain the reasoning behind NSA's redactions pursuant to Exemptions 1, 3, and 6,¹ and NSA's rationale for withholding documents pursuant to Exemptions 1 and 3. Finally, I will explain that NSA can neither confirm nor deny the existence of intelligence records responsive to Plaintiff's second FOIA request, as doing so would reveal information that is both currently and properly classified in accordance with E.O. 13526 as well as protected from disclosure by statute. Specifically, the

¹ Although NSA asserted Exemption 5 in the response letter, after further review, I have determined that Exemption 5 was inappropriate. Nonetheless, much of the information was properly redacted under Exemptions 1 and 3 pursuant to Section 6 of the National Security Agency Act of 1959 (Pub. L. No. 86-36, codified at 50 U.S.C. § 3605). NSA has prepared a reissuance of the documents with the proper redactions cited, contained in Exhibit F.

NSA cannot acknowledge the existence or nonexistence of intelligence information requested by Plaintiff because it is properly exempt from disclosure under the FOIA based upon Exemptions 1 and 3, 5 U.S.C. §§ 552(b)(1) and (3), respectively. This is because such a positive or negative response would reveal information that is currently and properly classified in accordance with E.O. 13526 and protected from release by statutes, specifically Section 6 of the National Security Agency Act of 1959 (Pub. L. No. 86-36, codified at 50 U.S.C. § 3605), 18 U.S.C. § 798, and Section 102(A)(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (codified at 50 U.S.C. § 3024).

I. NSA's ORIGIN AND MISSIONS

5. The NSA was established by Presidential Directive in October 1952 as a separately-organized agency within the Department of Defense (“DoD”) under the direction, authority, and control of the Secretary of Defense. NSA has two primary missions: (1) to collect, process, analyze, produce, and disseminate SIGINT information for foreign intelligence and counterintelligence purposes to provide support for national and departmental requirements and for conducting military operations; and (2) to conduct information assurance/cybersecurity activities. SIGINT involves collecting foreign intelligence from communications and information systems, including foreign communications, radar and other electronic systems.

6. NSA has developed a sophisticated worldwide SIGINT collection network that acquires foreign signals. In performing its SIGINT mission, NSA exploits foreign signals to obtain intelligence information necessary to the national defense, national security, and/or the conduct of foreign affairs. The technological infrastructure that supports NSA's SIGINT collection network has taken years to develop at a cost of billions of dollars and significant

human effort. It relies on sophisticated collection and processing technologies designed to keep pace with challenging new technological developments.

II. IMPORTANCE OF SIGINT TO THE NATIONAL SECURITY

7. There are two primary reasons for gathering and analyzing intelligence information. The first, and most important, is to gain the information required to direct U.S. resources as necessary for the national security of the United States. SIGINT information provided by the NSA is routinely distributed to a wide variety of senior Government officials, including the President, the President's National Security Advisor, the Director of National Intelligence, the Secretaries of Defense, State, Treasury, and Commerce, U.S. ambassadors serving in posts abroad, the Joint Chiefs of Staff, and the Unified and Specified Commanders. In addition, SIGINT information is disseminated to numerous agencies and departments including, among others, the Central Intelligence Agency ("CIA"), the Federal Bureau of Investigation ("FBI"), the Drug Enforcement Administration ("DEA"), the Departments of the Army, Navy, and Air Force, and various intelligence components of DoD. Information provided by NSA in a classified setting to the military and other government agencies and officials within the Intelligence Community ("IC") is relevant to a wide range of important issues including, but not limited to, military order of battle, threat warnings and readiness, arms proliferation, terrorism, and foreign aspects of international narcotics trafficking. This sensitive information is often critical to the conduct of U.S. foreign policy and of U.S. military operations around the world. Moreover, intelligence produced by NSA is often unobtainable by other means.

8. NSA's ability to produce SIGINT depends on its access to foreign signals. Further, SIGINT capabilities are both expensive and fragile. Public disclosure of either the

capability to collect specific signals or the substance of the SIGINT information itself can easily alert foreign adversaries to the vulnerability of their signals.

9. The subset of SIGINT information obtained from intercepted foreign communications is called communications intelligence (“COMINT”). A fundamental tenet of the COMINT process is that the identity of specific communicants whose communications are intercepted (commonly referred to as “targets”), the degree of success in exploiting these targets, and the vulnerability of particular foreign communications are all matters that must be maintained in strictest secrecy because the ability to exploit foreign communications is fragile. Disclosure of the identity of the targets, the ability to exploit those targets, or the vulnerability of particular foreign communications would encourage countermeasures by the targets of NSA’s COMINT efforts. Disclosure of even a single intercepted communication holds the potential to reveal the intelligence collection techniques that are applied against targets around the world. Once alerted, COMINT targets may change the way they communicate, which could inhibit access to the targets’ communications and, therefore, deny the United States access to information crucial to the defense of the United States both at home and abroad. If a target is successful in defeating an intercept operation, all of the intelligence from that source is lost unless and until NSA can establish new and equivalent exploitation of that target’s signals. If a source becomes unavailable, the military, national policymakers, combatant commanders, and the IC must operate without the information the communications provided. Such losses are extremely harmful to the national security of the United States.

10. Congress has specifically recognized the inherent sensitivity of the SIGINT activities of the NSA; thus, Congress has passed statutes to protect NSA’s SIGINT efforts from damage by disclosure. These statutes recognize the vulnerability of SIGINT to countermeasures

of a foreign power or terrorist party and the significance of the loss of valuable foreign intelligence information to national policymakers, combatant commanders, and the IC. These statutes are: Section 6 of the National Security Act of 1959 (codified at 50 U.S.C. § 3605); Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (codified at 50 U.S.C. § 3024); and 18 U.S.C. § 798. Under these three statutes, NSA is specifically authorized to protect certain information concerning its activities and its intelligence sources and methods from public disclosure.

III. PLAINTIFF'S FOIA REQUESTS

11. Plaintiff submitted two FOIA requests to NSA's FOIA Office. First, on October 29, 2018, Plaintiff submitted a request seeking "All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing" twelve individuals and/or entities: Seth Conrad Rich, Julian Assange, Wikileaks, Kim Dotcom, Aaron Rich, Shawn Lucas, Kelsey Mulka, Imran Iwan, Abid Awan, Jaman Awan, Hina Alvi, and Rao Abbas. Second, on June 12, 2020, Plaintiff submitted a request seeking the following three categories of records:

1. I request the opportunity to view all metadata, communications (internal or external), records documents, reports or other evidence regarding whether the National Security Agency ("NSA"), the Central Intelligence Agency ("CIA"), any "Five Eyes" allies, and/or affiliates, agents, employees or contractors of those agencies or any other government entity played a role in inserting Russian "fingerprints" (e.g., "COZY BEAR" or "FANCY BEAR") into data from the 2016 Data Breach. In other words, the NSA should produce all evidence indicating whether any U.S. Government or "Five Eyes" entities, affiliates, agents, employees or contractors inserted or fabricated evidence to make it appear that Russians or other third parties were responsible for the 2016 Data Breach. This includes, for example, any and all evidence that U.S. Government or "Five Eyes" entity, affiliate, agent, employee, or contractor created or operated the "Guccifer 2.0" or "DCLeaks" profiles or any other online profile used to promote or distributed data from the 2016 Data Breach.

2. I request the opportunity to view all tangible evidence reflecting the person, persons, or entities involved in 2016 Data Breach. This request includes, but is

not limited to, evidence indicating whether the breach was the result of (1) outside forces (*e.g.*, Russian agents, Pakistani agents, etc.) who hacked the servers from a remote location or (2) an individual or individuals who were present at or inside DNC facilities and copied the data onto a storage device. If, for example, NSA intercepted or obtained any communications between Seth Rich and Julian Assange or Wikileaks (*e.g.*, from the United Kingdom's Government Communications Headquarters, or any other person or entity), then those communications should be produced. If the NSA has any evidence whatsoever that the DNC servers were hacked externally or that DNC data was leaked from an internal source, that evidence should be produced.

3. I request the opportunity to view all communications exchanged (either directly or indirectly) between Seth Conrad Rich ("Seth Rich") and/or Aaron Nathan Rich ("Aaron Rich") and the following: Julian Assange, Wikileaks, and/or any agents or representatives of Wikileaks.

A true and correct copy of these requests are attached as Exhibit A to my declaration.

12. In response to Plaintiff's October 29, 2018 request, NSA sent a letter on October 31, 2018, informing Plaintiff that the request was assigned "Case Number 105508," and that "[d]ue to a significant increase in the number of requests being received by this Agency, we are experiencing delays in processing." The letter stated that NSA would "begin to process [Plaintiff's] request and [would] respond to [him] again as soon as we are able." After Plaintiff filed the Complaint in this case, NSA conducted a search for responsive records and provided five records, totaling 13 pages, to Plaintiff. In a February 2, 2021 letter, NSA also explained that six records, which totaled 16 pages, were being withheld in their entirety under Exemptions 1, 3, 5, and 6 of the FOIA. First, the letter explained that because the information was currently and properly classified in accordance with E.O. 13526, it was exempt from disclosure based on Exemption 1. Second, the letter explained that the same information was also protected from release by statute, and thus also exempt from release based upon Exemption 3. Specifically, the letter cited three statutes applicable to the case: 18 U.S.C. § 798, 50 U.S.C. § 3024(i), and Section 6 of Public Law 86-36 (codified at 50 U.S.C. § 3605). Third, the letter stated that the information was being withheld under Exemption 5 because the information was protected by

deliberative process privilege.² Finally, the letter explained that individuals' personal information was being withheld under Exemption 6 because the individuals' privacy interests outweighed the public interest for the information. A true and correct copy of these letters are attached as Exhibit B to my declaration.

13. In response to Plaintiff's June 12, 2020 request, NSA sent a letter on June 19, 2020, informing Plaintiff that the request was assigned "Case Number 109745," and that "[d]ue to the COVID-19 pandemic, the NSA FOIA Office ha[d] adjusted its normal operations to balance the need of completing its mission as effectively and efficiently as possible with adherence to the recommended social distancing guidelines for the safety of our staff and the community." The letter explained that "[a]s a result, [Plaintiff] may experience a delay in receiving an initial acknowledgment as well as a substantive response to [his] FOIA request or appeal." On January 20, 2021, NSA sent Plaintiff a letter explaining that the fact of the existence or nonexistence of responsive records was currently and properly classified in accordance with E.O. 13526 and was thus exempt from disclosure based upon Exemption 1 of the FOIA. The letter further explained that the existence or nonexistence of the same information was also protected from release by statute, and thus also exempt from release based upon Exemption 3 of the FOIA. This response is commonly referred to as a *Glomar* response (hereinafter "*Glomar*"). Finally, the letter informed the Plaintiff of his right to appeal this determination. A true and correct copy of these letters are attached as Exhibit C to my declaration.

14. On February 11, 2021, after Plaintiff filed a Complaint in this case, Plaintiff sent a letter to the FOIA/PA Appeal Authority appealing NSA's January 20, 2021 denial letter. In the

² As previously noted, I have determined that applying Exemption 5 to the information was inappropriate, but the information was properly redacted under other FOIA exemptions.

appeal letter, Plaintiff stated that “Section 1.7 of Executive Order 13526 expressly prohibits the use of classification for purposes of concealing government misconduct or illegal activity. If government entities lied to Congress about the persons responsible for transferring emails from the Democratic National Committee to Wikileaks in 2016, *e.g.*, by shifting blame to Russian hackers rather than DNC employee Seth Rich, then classification of that information would be improper under EO 13526. Likewise, a *Glomar* response would be improper.” Plaintiff also stated that “[w]ith respect to the matters in Request No. 3, the NSA would be fully expected to intercept communications between the Rich brothers and any foreign entities such as Wikileaks, therefore disclosure of the contents of those communications would not reveal anything about collection methods that is not already known.” A true and correct copy of this letter is attached as Exhibit D to my declaration.

IV. PLAINTIFF’S OCTOBER 2018 FOIA REQUEST – NSA’S SEARCH FOR RESPONSIVE DOCUMENTS

15. As stated above, NSA conducted a search for responsive records. The Agency tasked its Legislative, State, Local, and Academic Engagement office (“LSLA”) to search its records. Personnel from NSA’s Office of General Counsel (“OGC”), in coordination with the FOIA Office, directed and assisted in the search for responsive records. NSA OGC, in coordination with the FOIA Office, determined that LSLA was the most likely NSA organization to possess responsive records, to the extent responsive records existed, and that no other components of NSA were reasonably likely to possess additional materials responsive to Plaintiff’s request.

16. In tasking this search, NSA OGC directed LSLA to search the office’s records in all places where records responsive to the October 2018 FOIA request were most likely to be found. NSA OGC recommended that LSLA search its records for “[e]ach of the 12 names as

written” and “[v]ariations on each of the 12 names including: last name only; first and last name; and first, middle (if known), and last name.”

17. After collecting potentially responsive records from LSLA, personnel from OGC conducted a first-level review of the materials to determine if they were, in fact, responsive to Plaintiff’s request. OGC personnel then conducted a second-level review of selected materials to determine, in certain instances, responsiveness, as well as segregability. Ultimately, OGC determined that there were eleven records responsive to Plaintiff’s October 2018 FOIA request.

18. OGC determined that five response documents were segregable, containing non-exempt material releasable to Plaintiff. In coordination with the FOIA Office, NSA redacted certain information from these documents, which is exempt from disclosure, as detailed below.

19. OGC also determined that six documents contained exempt material and were non-segregable. Therefore, NSA withheld those documents from Plaintiff in full for the reasons explained below.

20. The documents released to Plaintiff reflect (1) an April 4, 2018 letter from Senators Richard Burr and Mark Warner, Chairman and Vice-Chairman, respectively, of the Senate Select Committee on Intelligence (“SSCI”), to NSA Director Admiral Michael Rogers; (2) NSA’s responses to several Senators’ Questions for the Record (“QFRs”) following a February 13, 2018 open session SSCI Worldwide Threats Hearing; (3) NSA’s response to Senator Tom Cotton’s QFR following a February 13, 2018 closed session SSCI Worldwide Threats Hearing; (4) a letter from Senators Richard Burr and Mark Warner, Chairman and Vice-Chairman, respectively, of SSCI with several Senators’ QFRs following a February 13, 2018 open session SSCI Worldwide Threats Hearing; and (5) a letter from Senators Richard Burr and Mark Warner, Chairman and Vice-Chairman, respectively, of SSCI with Senator Tom Cotton’s

QFR following a February 13, 2018 closed session SSCI Worldwide Threats Hearing. Each record released to Plaintiff contains redactions. Those documents, as produced to Plaintiff, are attached as Exhibit E.

21. NSA identified and searched the NSA components that were likely to possess records responsive to the FOIA request, and identified and used search methods that were reasonably likely to identify all responsive NSA records. This approach resulted in the release of five documents to Plaintiff that were determined to contain segregable non-exempt information. Additional pages of responsive material were identified during the course of this search, and were determined by OGC personnel to contain non-segregable information that is both classified and protected from disclosure by statute.

REDACTED MATERIAL IN DOCUMENTS RELEASED TO PLAINTIFF IN PART IS PROTECTED FROM DISCLOSURE PURSUANT TO EXEMPTIONS 1, 3, AND 6

22. The redactions contained in the five documents released in part to Plaintiff underscore the segregability review in which NSA engaged during this process. The redactions were made pursuant to FOIA Exemptions 1, 3, and 6, as further detailed below.

23. Based on my position as the Chief of EGS, the Agency official responsible for the processing of all requests made pursuant to FOIA, I am confident in NSA's determination that the redacted information is exempt from disclosure pursuant to the FOIA and no more exempt, reasonably segregable material can be released.

FOIA Exemption 1

24. Section 552(b)(1) of the FOIA provides that the FOIA does not require the release of matters that are specifically authorized—under criteria established by an Executive Order—to be kept secret in the interest of the national defense or foreign policy and are in fact properly

classified pursuant to such Executive Order. The current Executive Order that establishes such criteria is E.O. 13526.

25. Section 1.1 of E.O. 13526 provides that information may be originally classified if: (1) an original classification authority is classifying the information; (2) the information is owned by, produced by or for, or is under the control of the government; (3) the information falls within one or more of the categories of information listed in section 1.4 of the Executive Order; and (4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, and the original classification authority is able to identify or describe the damage.

26. Section 1.4 of E.O. 13526 provides that information shall not be considered for classification unless it falls within one (or more) of eight specifically enumerated categories of information. The categories of classified information at issue here are found in Section 1.4(c), which includes intelligence activities (including covert action), intelligence sources and methods, or cryptology.

27. The release of the redacted material would disclose information that is currently and properly classified TOP SECRET pursuant to Section 1.2(a)(1) of E.O. 13526, because the information could reasonably be expected to cause exceptionally grave damage to the national security. Any disclosure of this information would obviously and immediately affect the ability of NSA to counter threats to the national security of the United States.

28. In my role as a TOP SECRET OCA, I am authorized to make classification decisions at the TOP SECRET, SECRET, and CONFIDENTIAL levels. As set out below, I reviewed the categories of redacted information pursuant to this FOIA request and determined that those categories are currently and properly classified in accordance with E.O. 13526. Based

on that determination, I have further determined that the responsive material at issue was properly redacted, as this information is currently and properly classified in accordance with E.O. 13526. Accordingly, the release of this intelligence information could reasonably be expected to cause exceptionally grave damage to the national security. The damage to national security that reasonably could be expected to result from the unauthorized disclosure of this classified information is described below. Finally, in accordance with Section 1.7 of E.O. 13526, no information was classified or withheld in order to conceal violation of law, or to prevent embarrassment to the Agency.

29. Here, the redacted information is currently and properly classified.³ In fact, these redactions protect information that is classified as TOP SECRET, underscoring the exceptionally grave damage that would be implicated by its release. These redactions protect specific information concerning and derived from NSA SIGINT reporting, which plainly cannot be released to the public without exceptionally grave damage to national security. This redacted information, if revealed, would show specific topics that are the subject of NSA SIGINT reports. These intelligence reports are some of the most closely held and protected products that NSA creates, and cannot be disclosed without risk to national security given the insights they provide.

FOIA Exemption 3

30. Section 552(b)(3) of the FOIA provides that the FOIA does not require the disclosure of matters that are specifically exempted from disclosure by statute, provided that such statute requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or establishes particular criteria for withholding or refers to particular

³ Exemption 1 is cited on Bates Stamp pages TTP NSA 000007 and TTP NSA 000013. See Exhibit E at 7, 13. NSA's response to QFR 11 on Bates Stamp page TTP NSA 000005 is also classified, despite the absence of a (b)(1) citation. This is reflected in the documents that were prepared for reissuance to the Plaintiff.

types of matters to be withheld. *See* 5 U.S.C. § 552(b)(3). Review of the application of this section of the FOIA consists solely of determining that the statute relied upon qualifies as an exempting statute under Exemption 3 and that the information withheld falls within the scope of the statute. No showing of national security harm is required in order to maintain a proper exemption pursuant to Exemption 3.

31. The redacted material subject to this exemption plainly falls within NSA's unique statutory privilege: Section 6 of the National Security Agency Act of 1959, 50 U.S.C. § 3605. As noted, Section 6 is a statutory privilege unique to NSA and provides that "[n]othing in this chapter or any other law... shall be construed to require the disclosure of the organization or any function of the National Security Agency, or any information with respect to the activities thereof, or of the names, titles, salaries, or number of the persons employed by such agency." By this language, Congress expressed its finding that disclosure of any information relating to NSA activities is potentially harmful. The protection provided by this statute is, by its very terms, absolute, as Section 6 states unequivocally that, notwithstanding any other law, including the FOIA, NSA cannot be compelled to disclose any information with respect to its activities. Further, NSA is not required to demonstrate specific harm to national security when invoking this statutory privilege, rather, NSA need only to show that the information falls within the scope of Section 6. NSA's organization, functions, activities, and nonpublic personnel are therefore protected from disclosure regardless of whether or not the information is classified.

32. Here, NSA has redacted certain information relating to NSA's functions and activities pursuant to Exemption 3.⁴ As explained, these redactions protect information

⁴ Exemption 3 is cited on Bates Stamp pages TTP NSA 00001, 000002, 000003, 000007 and 000013. *See* Exhibit E at 1, 2, 7, 13. NSA's responses to QFR 11 and 12, on Bates Stamp pages TTP NSA 000005 and TTP NSA 000006 are also protected by Exemption 3 pursuant to Section 6, despite the absence of a (b)(3)

concerning and derived from NSA SIGINT reporting. Collecting intelligence information and providing it to principals, advisors, and leaders in the United States government, including Congressional oversight committees, is a core function and primary activity of NSA. Additionally, these redactions protect information revealing NSA's intelligence assessments, another central function and activity of NSA. Finally, these redactions protect information describing NSA's role in the Vulnerabilities Equities Process ("VEP") that have not been publicly acknowledged. The details of NSA's involvement in the VEP is also an NSA function/activity. Congress's intent with respect to the protection of NSA's organization, functions, and activities is manifest by the plain language of Section 6; where, as here, the disclosure of the requested information would improperly reveal aspects of NSA's mission, the invocation of Exemption 3 pursuant to this statute is proper.

33. NSA also redacted the standard identifier of an NSA employee pursuant to Exemption 3. NSA employees' standard identifiers contain some or all of a particular employee's name. NSA protects the standard identifiers of its personnel pursuant to Section 6, which, as noted, protects from disclosure the organization of NSA and the names and titles of those employed with NSA. This material is appropriately redacted pursuant to Exemption 3 of the FOIA, as it reflects information that squarely falls within the express protections of Section 6.

34. Based upon my review, I therefore conclude that this material is appropriately redacted pursuant to Exemption 3 of the FOIA, as it reflects information that squarely falls within the express protections of Section 6.

citation. This is reflected in the documents that were prepared for reissuance to the Plaintiff, and contained herein at Exhibit F.

FOIA Exemption 6

35. Lastly, section 552(b)(6) of the FOIA protects from disclosure information whose release would lead to a clearly unwarranted invasion of personal privacy. In order to determine whether material is properly withheld pursuant to this exemption, an agency must conduct a balancing test, weighing the public interest in disclosure versus the privacy interest at stake.

36. Here, a careful examination of the redacted material reveals that the public interest in disclosure is minimal and clearly outweighed by the privacy interest involved. Specifically, the only material redacted pursuant to Exemption 6 contains the full names and phone numbers of members of the SSCI staff. There is no public interest in the release of these staff members' personal information, specifically their names and phone numbers. These individuals have an obvious privacy interest in their personal information.

**MATERIALS WITHHELD IN FULL ARE PROTECTED FROM DISCLOSURE
PURSUANT TO EXEMPTIONS 1 AND 3**

37. In addition to the redacted material on the five documents released in part, NSA also withheld from disclosure six documents, totaling 16 pages, pursuant to Exemptions 1 and 3. Most, if not all, of this material is classified and non-segregable for that reason alone, as described in further detail below, and thus NSA is unable to produce any non-exempt portions of the responsive materials. In sum, I have reviewed the material withheld in full and determined that no reasonably segregable portions can be released.

FOIA Exemption 1

38. As explained above, section 552(b)(1) of the FOIA provides that the FOIA does not require the release of matters that are specifically authorized—under criteria established by an Executive Order—to be kept secret in the interest of the national defense or foreign policy and

are in fact properly classified pursuant to such Executive Order. The current Executive Order that establishes such criteria is E.O. 13526.

39. Section 1.1 of E.O. 13526 provides that information may be originally classified if certain conditions are met. Those four conditions are outlined *supra* in paragraph 25.

40. Section 1.4 of E.O. 13526 provides that information shall not be considered for classification unless it falls within one (or more) of eight specifically enumerated categories of information. The categories of classified information at issue here are found in Section 1.4(c), which includes intelligence activities (including covert action), intelligence sources and methods, or cryptology. Disclosure of the withheld information would reveal information related to this category that is currently and properly classified as set forth in Section 1.4(c) of E.O. 13526.

41. The release of the material withheld in full would disclose information that is currently and properly classified TOP SECRET pursuant to Section 1.2(a)(1) of E.O. 13526, because the information could reasonably be expected to cause exceptionally grave damage to the national security. Any disclosure of this information would obviously and immediately affect the ability of NSA to counter threats to the national security of the United States.

42. In my role as a TOP SECRET OCA, I am authorized to make classification decisions at the TOP SECRET, SECRET, and CONFIDENTIAL levels. As set out below, I reviewed the categories of redacted information pursuant to this FOIA request and determined that those categories are currently and properly classified in accordance with E.O. 13526. Based on that determination, I have further determined that the responsive material at issue was properly withheld, as all of this information is currently and properly classified in accordance with E.O. 13526. Accordingly, the release of this information could reasonably be expected to cause exceptionally grave damage to the national security. The damage to national security that

reasonably could be expected to result from the unauthorized disclosure of this classified information is described below. Finally, in accordance with Section 1.7 of E.O. 13526, no information was classified or withheld in order to conceal violation of law, or to prevent embarrassment to the Agency.

43. All of the documents withheld in full by NSA are currently and properly classified. In fact, all of these documents are classified TOP SECRET,⁵ underscoring the exceptionally grave damage that would be implicated by their release. Moreover, I have determined that the classified material withheld in full does not contain meaningfully segregable information that could be released to the public. This is so for several reasons. First, in many instances, the withheld material does not contain any non-classified material. Second, even in those documents where there are stray lines containing unclassified or U//FOUO material, that material, without more, is not meaningful or substantive. Finally, these documents concern specific topics the very existence of which are classified. While NSA is prepared to state, on the public record, that it has withheld a specified number of materials responsive to Plaintiff's request, namely, "correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing" either Seth Conrad Rich, Julian Assange, Wikileaks, Kim Dotcom, Aaron Rich, Shawn Lucas, Kelsey Mulka, Imran Iwan, Abid Awan, Jamal Awan, Hina Alvi, or Rao Abbas, it cannot provide additional detail concerning the withheld material without risking exceptionally grave damage to national security.

⁵ In fact, many of these documents have additional classifications indicating the sensitivity of the material at issue. For example, many of the documents are marked with "ORCON" designator, indicating that the originator of the information controls to whom it is release. Additionally, all of the documents contain the designator "NOFORN," indicating that the information may not be released to foreign governments, foreign nationals, or non-U.S. citizens without permission of the originator and in accordance with DNI policy.

44. These documents contain information from intelligence reporting derived from SIGINT and associated analysis or explanation, which plainly cannot be released to the public without exceptionally grave damage to national security. The information from these intelligence reports, which are some of the most closely held and protected products that NSA creates, cannot be disclosed without risk to national security given the insights they provide.

45. All the documents withheld in full by NSA are classified at levels which, on their face, indicate the sensitivity of the at-issue material. Moreover, this classified material does not contain meaningfully segregable portions, and, in most instances the very existence of the specific material withheld is classified. Accordingly, while NSA may, without harm to national security, publicly state that it possesses material responsive to Plaintiff's FOIA request, it does not follow from that admission that NSA must in turn reveal classified details concerning such material.

FOIA Exemption 3

46. While, for the aforementioned reasons, the materials withheld in full are currently and properly classified and accordingly exempt from disclosure pursuant to Exemption 1, the Court need not consider the classification issue, as all requested records are concurrently exempt pursuant to Exemption 3. 5 U.S.C. § 552(b)(3).

47. The statutory language of 5 U.S.C. § 552(b)(3), and an explanation of the corresponding legal standard, is recited *supra* in paragraph 30, which I hereby incorporate by reference.

48. The information withheld in full here is protected from disclosure by several statutes. First and foremost, the withheld documents concern or reference NSA SIGINT information, which implicate both the Agency's core functions and activities, as well as

intelligences sources and methods. As such, they fall squarely within NSA's unique statutory privilege: Section 6 of the National Security Agency Act. Congress enacted this statute to protect the fragile nature of NSA's SIGINT efforts, including, but not limited to, the existence and depth of signal intelligence-related analytical successes, weaknesses, and exploitation techniques. This statute recognizes the vulnerability of SIGINT to countermeasures and the significance of the potential loss of valuable intelligence information to national policymakers, combatant commanders, and the IC.

49. The statutory language of Section 6, and an explanation of the corresponding legal standard, is recited *supra* in paragraph 31, which I hereby incorporate by reference.

50. In addition to the plainly applicable statutory framework of Section 6, the materials withheld in full also are protected from disclosure by 18 U.S.C. § 798. This statute prohibits the unauthorized disclosure of classified information: (i) concerning the communication intelligence activities of the United States, or (ii) obtained by the process of communication intelligence derived from the communications of any foreign government. The term "communication intelligence," as defined by Section 798, means the "procedures and methods used in the interception of communications and obtaining the information from such communications by other than the intended recipients." 18 U.S.C. § 798(b). As noted above, some of the withheld material implicates NSA's SIGINT information. This material, while classified, is also plainly protected by the strictures of § 798. This statutory scheme underscores Congress's commitment to protecting communication intelligence, which is central to NSA's mission, from disclosure. Here, given the classified nature of the withheld material, as well as its reflection of NSA's core activities, it is axiomatic that disclosure of the withheld information about this intelligence source (communication intelligence) and the related methods used to

secure it, would reveal critical information about the means through which NSA collects and processes communication intelligence, plainly falling within the scope of this statutory scheme.

51. Finally, the withheld material is protected from disclosure by Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. § 3024, which states that “[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure.” NSA, as a member agency of the U.S. IC, must also protect intelligence sources and methods. Like the protection afforded to core NSA activities by Section 6 of the NSA Act of 1959, the protection afforded to intelligence sources and methods is absolute. Whether the sources and methods at issue are classified is irrelevant for purposes of the protection afforded by 50 U.S.C. § 3024.

52. Here, the details of the withheld material responsive to Plaintiff’s request concerning correspondences with Congress regarding or referencing specific individuals implicates critical sources and methods. Detailed discussions about circulated intelligence reports and NSA capabilities, both of which generally describe the type of information present in these withheld materials, reflect the very sources and methods this statute is designed to protect.

53. Based upon my review, I therefore conclude that the records withheld in full are not only exempt from disclosure due to their classified nature, but also, in light of the fact that their contents are plainly protected from release by the aforementioned three statutory authorities: (1) Section 6, 50 U.S.C. § 3605, because the withheld information concerns the core function and/or activities of NSA; (2) 18 U.S.C. § 798, because disclosure could reveal classified information derived from NSA’s exploitation of foreign communications; and (2) Section 102A(i)(1), 50 U.S.C. § 3024, because the information concerns intelligence sources and

methods. For these reasons, all of the documents withheld in full are, in the alternative, protected from disclosure pursuant to Exemption 3.

V. PLAINTIFF'S JUNE 2020 FOIA REQUEST– NSA'S GLOMAR DETERMINATION

54. NSA interpreted Plaintiffs' request as one seeking intelligence records; specifically COMINT which includes intercepted foreign government communications. To the extent a Plaintiff seeks intelligence information, NSA's response is to state that it cannot confirm or deny publicly in any case whether or not it has such records, as doing so would reveal whether or not NSA engaged in certain, or any, intelligence activities, and/or did or did not target individual communications for collection.

55. Based upon my position as the Chief of EGS, the Agency official responsible for the processing of all requests made pursuant to FOIA, I am confident that NSA's determination that it could not acknowledge the existence or nonexistence of intelligence information was proper because a positive or negative response to such a request would reveal information that is currently and properly classified in accordance with E.O. 13526 and protected from disclosure by statute. I will explain how the requested information is currently and properly classified and how the statutory exemptions were properly applied.

**INFORMATION ABOUT NSA SIGINT ACTIVITIES IS CLASSIFIED AND
THUS FALLS UNDER FOIA EXEMPTION 1**

56. Section 552(b)(1) of the FOIA provides that the FOIA does not require the release of matters that are specifically authorized—under criteria established by an Executive Order – to be kept secret in the interest of the national defense or foreign policy and are in fact properly classified pursuant to such Executive Order. The current Executive Order that establishes such criteria is E.O. 13526.

57. Section 1.1 of E.O. 13526 provides that information may be originally classified if certain conditions are met. Those four conditions are outlined *supra* in paragraph 25.

58. Section 1.4 of E.O. 13526 provides that information shall not be considered for classification unless it falls within one (or more) of eight specifically enumerated categories of information. The categories of classified information at issue here are found in Section 1.4(c), which includes intelligence activities (including covert action), intelligence sources and methods, or cryptology. Acknowledgment of the existence or nonexistence of operational intelligence information concerning the who, what, when, and how of NSA's SIGINT collection efforts would reveal information that is currently and properly classified as set forth in Sections 1.4(c) of E.O. 13526.

59. Confirming the existence or nonexistence of responsive records would disclose information that is currently and properly classified TOP SECRET pursuant to Section 1.2(a)(1), of E.O. 13526 because all of the information that Plaintiffs sought fall under one or more of the above referenced exceptions and therefore would remain classified to date. A positive or negative response to Plaintiffs' request reasonably could be expected to cause exceptionally grave damage to national security. Any disclosure of this information could reasonably be expected to harm national security because it would reveal NSA intelligence capabilities, activities, and priorities, which in turn could inhibit SIGINT collection and affect NSA's ability to counter threats to the national security of the United States.

60. Acknowledging the existence or nonexistence of responsive records on particular individuals or organizations that may be subject to surveillance would provide our adversaries with critical information about the capabilities and limitations of the NSA, such as the types of communications that may be susceptible to NSA detection. Confirmation by NSA that a

person's activities are not of foreign intelligence interest or that NSA is unsuccessful in collecting foreign intelligence information on their activities on a case-by-case basis would allow our adversaries to accumulate information and draw conclusions about NSA's technical capabilities, sources, and methods. For example, if NSA were to admit publicly in response to a FOIA request that no information about Persons X or Y exists, but in response to a separate FOIA request about Person Z state only that no response could be made, this would give rise to the inference that Person Z is or has been a target. Over time, the accumulation of these inferences would disclose the targets and capabilities, and therefore the sources and methods, of NSA's SIGINT activities and functions, and inform our adversaries of the degree to which NSA is aware of some of their operatives or can successfully exploit particular communications.

61. NSA cannot respond to each case in isolation, but must assume that our adversaries will examine all released information together. These compilations of information, if disclosed, could reasonably be expected to cause exceptionally grave and irreparable damage to the national security by providing our adversaries a road map that instructs them on which communication modes or personnel remain safe or are successfully defeating NSA's capabilities. Our adversaries could exploit this information in order to conduct their activities more securely, to the detriment of the national security of the United States. Indeed, section 1.7(e) of E.O. 13526 specifically contemplates the danger of such compilations.

62. Therefore, the NSA must use the *Glomar* response consistently in all cases where the existence or nonexistence of records responsive to a FOIA request is a classified fact, including in both instances in which the NSA does or does not possess records responsive to a particular request. If the NSA were to invoke a *Glomar* response only when it actually possessed

responsive records, the *Glomar* response would be interpreted as an admission that responsive records exist. Consistent use of the *Glomar* response is necessary to ensure its effectiveness.

63. NSA's determination that the existence or nonexistence of the requested records is classified has not been made to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interests of national security.

64. For these reasons, the fact of the existence or nonexistence of intelligence information requested by Plaintiffs is a currently and properly classified matter in accordance with E.O. 13526, and thus Plaintiff's FOIA request was properly denied pursuant to FOIA Exemption 1.

**INFORMATION ABOUT NSA SIGINT ACTIVITIES IS PROTECTED FROM
DISCLOSURE BY STATUTE AND THUS FALLS UNDER FOIA EXEMPTION 3**

65. The statutory language of Exemption 3, and an explanation of the corresponding legal standard, is recited *supra* in paragraph 30, which I hereby incorporate by reference.

66. The information at issue here falls squarely within the scope of several statutes. Information about NSA's SIGINT efforts directly relates to the Agency's core functions and activities and to intelligence sources and methods. As described above, Congress enacted three statutes to protect NSA's SIGINT efforts against disclosure, including but not limited to the existence and depth of signals intelligence-related successes, weaknesses, and exploitation techniques. These statutes recognize the vulnerability of signals intelligence to countermeasures and the significance of the loss of valuable intelligence information to national policymakers, combatant commanders, and the IC.

67. The first of these statutes is Section 6 of the National Security Agency Act of 1959, 50 U.S.C. § 3605. The statutory language of Section 6, and an explanation of the corresponding legal standard, is recited *supra* in paragraph 31, which I hereby incorporate by reference.

68. The second applicable statute is 18 U.S.C. § 798. The statutory language of Section 798, and an explanation of the corresponding legal standard, is recited *supra* in paragraph 50, which I hereby incorporate by reference.

69. The third applicable statute is the National Security Act of 1947, as amended by the Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. § 3024. The statutory language of Section 798, and an explanation of the corresponding legal standard, is recited *supra* in paragraph 51, which I hereby incorporate by reference.

70. As described above, Congress has enacted these three statutes to protect NSA's SIGINT efforts against disclosure. Given that through these statutes Congress specifically prohibited the disclosure of information related to NSA's functions and activities and its communications intelligence activities, as well as the sources and methods used by the IC as a whole, I have determined that NSA's SIGINT activities and functions, and its intelligence sources and methods, would be revealed if NSA confirmed or denied the existence of information responsive to Plaintiff's FOIA request. If NSA were to admit the existence or non-existence of the requested records, the very information that Congress authorized NSA to protect would be revealed and this release could show the classified functions, communications intelligence activities, and sources and methods of NSA.

71. Based upon my review, I therefore conclude that the acknowledgment of the existence or nonexistence of intelligence information requested by Plaintiff is protected from

disclosure by statute pursuant to the following three authorities: (1) Section 6 of the National Security Act of 1959, 50 U.S.C. § 3605, because the information concerns the organization, function, and activities of the NSA as described above; (2) 18 U.S.C. § 798, because disclosure would reveal classified information derived from NSA's exploitation of foreign communications; and (3) Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. § 3024, because the information concerns intelligence sources and methods. For these reasons, acknowledgement of the existence or nonexistence of intelligence information requested by Plaintiffs is prohibited by statute and has been properly determined to be exempt from disclosure pursuant to the FOIA. Accordingly, the *Glomar* response is proper based on Exemption 3 of the FOIA, but this same response is also warranted based on Exemption 1, as set forth above.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 10th day of February, 2022, pursuant to 28 U.S.C. § 1746.

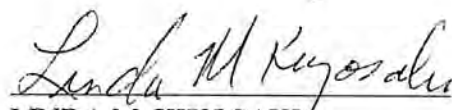

LINDA M. KIYOSAKI
Chief of Enterprise Guidance Services
National Security Agency

EXHIBIT A

Archer, Lynn M

From: donotreply@nsa.gov
Sent: Monday, October 29, 2018 1:36 PM
To: FOIANET
Subject: Message from FOIA Request Form

Your Name: Mr. Ty O Clevenger
Email Address: tyclevenger@yahoo.com
Company/Organization: The Transparency Project
P.O. Box 20753
Postal Address: Brooklyn NY US 11202-0753
Home Phone: 9799855289
Work Phone:

Describe the records you seek, and provide any additional pertinent information (up to 5000 characters):

In response to the October 4, 2018 letter that I received regarding FOIA Request No. 102706B, I wish to submit a new FOIA request on behalf of The Transparency Project. In particular, I request:

1. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Seth Conrad Rich.
2. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Julian Assange.
3. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Wikileaks.
4. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Kim Dotcom.
5. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Aaron Rich.
6. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Shawn Lucas.
7. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Kelsey Mulka.
8. All correspondence received from or sent to any member of Congress (or

anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Imran Iwan.

9. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Abid Awan.

10. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Jamal Awan.

11. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Hina Alvi.

12. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Rao Abbas.

Each of the numbered items above should be considered a separate request.

The Transparency Project is a nonprofit Texas corporation and intends to use all of the information requested above to educate the public about government misconduct, therefore I request a waiver of any fees. If charges will apply, please let me know the approximate amount of such charges in advance. I can be reached by email at tyclevenger@yahoo.com if you need additional information.

Date Range of Requested Documents

January 1, 2016 until present.

HTTP_CMS_CLIENT_IP:
HTTP_X_ARR_LOG_ID: 49b79816-6d4a-4f80-884a-0392364b89f5
HTTP_ORIGIN: <https://www.nsa.gov>
HTTP_TRUE_CLIENT_IP: 100.33.243.17

RECEIVED 15 JUNE 2020

THE TRANSPARENCY PROJECT

P.O. Box 20753
Brooklyn, New York 11202
(979) 985-5289

June 12, 2020

National Security Agency
FOIA Requester Service Center
9800 Savage Road, Suite 6932
Ft. George G. Meade, MD 20755-6932
foiarsc@nsa.gov

Re: Freedom of Information Act Request

To Whom It May Concern:

I write on behalf of The Transparency Project ("TTP"), a nonprofit corporation headquartered in Texas, to request information about the removal, transfer, copying or stealing of data from Democratic National Committee (hereinafter "DNC") computer servers in 2016, data which was later published by Wikileaks.¹ That event will hereinafter be referred to as the "2016 Data Breach." I make these requests under the authority of the Freedom of Information Act, 5 U.S.C. § 552.

1. I request the opportunity to view all metadata, communications (internal or external), records, documents, reports or other evidence regarding whether the National Security Agency ("NSA"), the Central Intelligence Agency ("CIA"), any "Five Eyes" allies, and/or affiliates, agents, employees or contractors of those agencies or any other government entity played a role in inserting Russian "fingerprints" (e.g., "COZY BEAR" or "FANCY BEAR") into data from the 2016 Data Breach. In other words, the NSA should produce all evidence indicating whether any U.S. Government or "Five Eyes" entities, affiliates, agents, employees or contractors inserted or fabricated evidence to make it appear that Russians or other third parties were responsible for the 2016 Data Breach. This includes, for example, any and all evidence that U.S. Government or "Five Eyes" entity, affiliate, agent, employee, or contractor created or operated the "Guccifer 2.0" or "DCLeaks" profiles or any other online profile used to promote or distribute data from the 2016 Data Breach.
2. I request the opportunity to view all tangible evidence reflecting the person, persons, or entities involved in 2016 Data Breach. This request includes, but is not limited to, evidence indicating whether the breach was the result of (1) outside forces (e.g., Russian agents, Pakistani agents, etc.) who hacked the servers from a remote location or (2) an individual or individuals who were present at or inside DNC facilities and copied the data onto a storage device. If, for example, NSA intercepted or obtained any communications between Seth Rich and Julian Assange or Wikileaks (e.g., from the United Kingdom's Government

¹ The following terms or their derivatives are used interchangeably in this subpoena when referring to the movement of the relevant DNC data: leak, hack, remove, transfer, copy, or steal.

Communications Headquarters, or any other person or entity), then those communications should be produced. If the NSA has any evidence whatsoever that the DNC servers were hacked externally or that DNC data was leaked from an internal source, that evidence should be produced.

3. I request the opportunity to view all communications exchanged (either directly or indirectly) between Seth Conrad Rich ("Seth Rich") and/or Aaron Nathan Rich ("Aaron Rich") and the following: Julian Assange, Wikileaks, and/or any agents or representatives of Wikileaks.

The foregoing requests should be construed to cover all data, records, information, and tangible evidence in the possession or control of NSA, including information that was originally obtained by another entity such as the United Kingdom's Government Communications Headquarters.

TTP intends to use the requested information to educate the public about the prevalence of misconduct in the CIA, therefore I request a waiver of any fees. If charges will apply, please let me know the approximate amount of such charges in advance. I can be reached by email at tyclevenger@yahoo.com if you need additional information.

Sincerely,



Ty Clevenger
Executive Director

EXHIBIT B



NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 105508
31 October 2018

TY CLEVENGER
THE TRANSPARENCY PROJECT
PO BOX 20753
BROOKLYN NY 11202-0753

Dear Mr. Clevenger:

This is an initial response to your Freedom of Information Act (FOIA) request dated 29 October 2018, which was received by this office on 29 October 2018 for:

1. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Seth Conrad Rich.
2. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Julian Assange.
3. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Wikileaks.
4. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Kim Dotcom.
5. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Aaron Rich.
6. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Shawn Lucas.
7. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Kelsey Mulka.
8. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Irman Iwan.

FOIA Case: 105508

9. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Abid Awan.
10. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Jamal Awan.
11. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Hina Alvi.
12. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Rao Abbas.

Each of the numbered items above should be considered a separate request.
Date range of requested documents is January 1, 2016 until present.

This letter acknowledges that we have received your request and provides some administrative information. Your request has been assigned Case Number 105508. Due to a significant increase in the number of requests being received by this Agency, we are experiencing delays in processing. We will begin to process your request and will respond to you again as soon as we are able. Once we have completed a thorough review of your request, we will contact you should we require further clarification of your request. Until further processing is done, we do not know if there will be assessable fees. Therefore, we have not addressed your request for a fee waiver at this time.

Correspondence related to your request should include the case number assigned to your request, which is included in the first paragraph of this letter. Your letter should be addressed to National Security Agency, FOIA Office (P132), 9800 Savage Road STE 6932, Ft. George G. Meade, MD 20755-6932 or may be sent by facsimile to 443-479-3612. If sent by fax, it should be marked for the attention of the FOIA office. The telephone number of the FOIA office is 301-688-6527.

Sincerely,

Mike S.

FOIA Customer Representative



NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 105508A
2 February 2021

TY CLEVENGER
THE TRANSPARENCY PROJECT
PO BOX 20753
BROOKLYN NY 11202-0753

Dear Ty Clevenger :

This responds to your Freedom of Information Act (FOIA) request of 29 October 2018 for the twelve items listed below:

1. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Seth Conrad Rich.
2. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Julian Assange.
3. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Wikileaks.
4. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Kim Dotcom.
5. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Aaron Rich.
6. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Shawn Lucas.

FOIA Case: 105508A

7. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Kelsey Mulka.
8. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Imran Iwan.
9. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Abid Awan.
10. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Jamal Awan.
11. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Hina Alvi.
12. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Rao Abbas.

A copy of your request is enclosed. Your request has been processed under the FOIA and some of the documents you requested are enclosed. Certain information, however, has been withheld from the enclosures and six documents (16 pages) have been protected in their entirety.

Some of the withheld information has been found to be currently and properly classified in accordance with Executive Order 13526. The information meets the criteria for classification as set forth in Subparagraph (c) of Section 1.4 and remains classified TOP SECRET. The information is classified because its disclosure could reasonably be expected to cause exceptionally grave damage to the national security. Because the information is currently and properly classified, it is exempt from disclosure pursuant to the first exemption of the FOIA (5 U.S.C. Section 552(b)(1)).

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. We have determined that such information exists in these documents. Accordingly, those portions are exempt from disclosure pursuant to the third exemption of the FOIA, which provides for the withholding of information specifically protected from disclosure by statute. The specific statutes applicable in this case are Title 18 U.S. Code

FOIA Case: 105508A

798; Title 50 U.S. Code 3024(i); and Section 6, Public Law 86-36 (50 U.S. Code 3605).

Information also has been withheld from the enclosures pursuant to the fifth exemption of the FOIA. This exemption applies to inter-agency or intra-agency memoranda or letters that would not be available by law to a party other than an agency in litigation with the agency, protecting information that is normally privileged in the civil discovery context, such as information that is part of a predecisional deliberative process.

Lastly, personal information regarding individuals has been withheld from the enclosures in accordance with 5 U.S.C. 552 (b)(6). This exemption protects from disclosure information that would constitute a clearly unwarranted invasion of personal privacy. In balancing the public interest for the information you request against the privacy interests involved, we have determined that the privacy interests sufficiently satisfy the requirements for the application of the (b)(6) exemption.

Sincerely,

A handwritten signature in black ink, appearing to read 'RM' followed by a stylized flourish.

RONALD MAPP
Chief, FOIA/PA Office
NSA Initial Denial Authority

Encls:
a/s

EXHIBIT C



NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 109745
19 June 2020

TY CLEVENGER
THE TRANSPARENCY PROJECT
PO BOX 20753
BROOKLYN, NY 11202-0753

Dear Ty Clevenger:

This is an initial response to your Freedom of Information Act (FOIA) request dated 12 June 2020, received in this office on 15 June 2020, for "...information about the removal, transfer, copying or stealing of data from Democratic National Committee (hereinafter "DNC") computer servers in 2016, data which was later published by Wikileaks. That event will hereinafter be referred to as the "2016Data Breach." I make these requests under the authority of the Freedom of Information Act, 5U. S.C. § 552.

1. I request the opportunity to view all metadata, communications (internal or external), records, documents, reports or other evidence regarding whether the National Security Agency ("NSA"), the Central Intelligence Agency ("CIA"), any "Five Eyes" allies, and/or affiliates, agents, employees or contractors of those agencies or any other government entity played a role in inserting Russian "fingerprints" (e.g., "COZY BEAR" or "FANCYBEAR") into data from the 2016 Data Breach. In other words, the NSA should produce all evidence indicating whether any U.S. Government or "Five Eyes" entities, affiliates, agents, employees or contractors inserted or fabricated evidence to make it appear that Russians or other third parties were responsible for the 2016 Data Breach. This includes, for example, any and all evidence that U.S. Government or "Five Eyes" entity, affiliate, agent, employee, or contractor created or operated the "Guccifer 2.0" or "DCLeaks" profiles or any other online profile used to promote or distribute data from the 2016 Data Breach.

2. I request the opportunity to view all tangible evidence reflecting the person, persons, or entities involved in 2016 Data Breach. This request includes, but is not limited to, evidence indicating whether the breach was the result of (1) outside forces (e.g., Russian agents, Pakistani agents, etc.) who hacked the servers from a remote location or (2) an individual or individuals who were present at or inside DNC facilities and copied the data onto a storage device. If, for example, NSA intercepted or obtained any communications between Seth Rich and Julian Assange or Wikileaks (e.g., from the United Kingdom's Government Communications Headquarters, or any other person or entity), then those communications should be produced. If the NSA has any evidence whatsoever that the DNC servers were hacked externally or that DNC data was leaked from an internal source, that evidence should be produced.

FOIA Case: 109745

3. I request the opportunity to view all communications exchanged (either directly or indirectly) between Seth Conrad Rich ("Seth Rich") and/or Aaron Nathan Rich ("Aaron Rich") and the following: Julian Assange, Wikileaks, and/or any agents or representatives of Wikileaks.

This letter acknowledges that we have received your request and provides some administrative information. Your request has been assigned Case Number 109745. Due to the COVID-19 pandemic, the NSA FOIA Office has adjusted its normal operations to balance the need of completing its mission as effectively and efficiently as possible with adherence to the recommended social distancing guidelines for the safety of our staff and the community. As a result, you may experience a delay in receiving an initial acknowledgement as well as a substantive response to your FOIA request or appeal. You may reach out to our FOIA Requester Service Center (foiarsc@nsa.gov) and FOIA Public Liason (foialo@nsa.gov) if you have any questions about your request. We apologize for this inconvenience and appreciate your understanding and patience.

Until further processing is done, we do not know if there will be assessable fees. Therefore, we have not addressed your fee category.

Correspondence related to your request should include the case number assigned to your request, which is included in the first paragraph of this letter. Your letter should be addressed to National Security Agency, FOIA Office (P132), 9800 Savage Road STE 6932, Ft. George G. Meade, MD 20755-6932 or may be sent by facsimile to 443-479-3612. If sent by fax, it should be marked for the attention of the FOIA office. The telephone number of the FOIA office is 301-688-6527.

Sincerely,

A handwritten signature in black ink, appearing to read "Andrew F.", is positioned above the title "FOIA Customer Representative".

FOIA Customer Representative



NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 109745

TY CLEVENGER
THE TRANSPARENCY PROJECT
PO BOX 20753
BROOKLYN NY 11202-0753

Dear Ty Clevenger:

This responds to your Freedom of Information Act (FOIA) request of 12 June 2020, which was received by this office on 15 June 2020, for:

1. "I request the opportunity to view all metadata, communications (internal or external), records, documents, reports or other evidence regarding whether the National Security Agency ('NSA'), the Central Intelligence Agency ("CIA"), any "Five Eyes" allies, and/or affiliates, agents, employees or contractors of those agencies or any other government entity played a role in inserting Russian 'fingerprints' (e.g., 'COZY BEAR' or 'FANCYBEAR') into data from the 2016 Data Breach. In other words, the NSA should produce all evidence indicating whether any U.S. Government or 'Five Eyes' entities, affiliates, agents, employees or contractors inserted or fabricated evidence to make it appear that Russians or other third parties were responsible for the 2016 Data Breach. This includes, for example, any and all evidence that U.S. Government or 'Five Eyes' entity, affiliate, agent, employee, or contractor created or operated the 'Guccifer 2.0' or 'DCLeaks' profiles or any other online profile used to promote or distribute data from the 2016 Data Breach."
2. "I request the opportunity to view all tangible evidence reflecting the person, persons, or entities involved in 2016 Data Breach. This request includes, but is not limited to, evidence indicating whether the breach was the result of (1) outside forces (e.g., Russian agents, Pakistani agents, etc.) who hacked the servers from a remote location or (2) an individual or individuals who were present at or inside DNC facilities and copied the data onto a storage device. If, for example, NSA intercepted or obtained any communications between Seth Rich and Julian Assange or Wikileaks (e.g., from the United Kingdom's Government Communications Headquarters, or any other person or entity), then those communications should be produced. If the NSA has any evidence whatsoever that the DNC servers were hacked externally or that DNC data was leaked from an internal source, that evidence should be produced."
3. "I request the opportunity to view all communications exchanged (either directly or indirectly) between Seth Conrad Rich ('Seth Rich') and/or Aaron

FOIA Case: 109745

Nathan Rich ('Aaron Rich') and the following: Julian Assange, Wikileaks, and/or any agents or representatives of Wikileaks."

Your letter has been assigned Case Number 109745. Please refer to this case number when contacting us about your request. There are no assessable fees for this request; therefore, we did not address your fee category. Your request has been processed under the provisions of the FOIA.

NSA collects and provides intelligence derived from foreign communications to policymakers, military commanders, and law enforcement officials. We do this to help these individuals protect the security of the United States, its allies, and their citizens from threats such as terrorism, weapons of mass destruction, foreign espionage, international organized crime, and other hostile activities. What we are authorized to do, and how we do it, is described in Executive Order 12333. Information about how NSA conducts signals intelligence activities is available on the websites of NSA (www.nsa.gov) and the Office of the Director of National Intelligence (www.dni.gov).

We have determined that the fact of the existence or non-existence of the materials you request is a currently and properly classified matter in accordance with Executive Order 13526, as set forth in Subparagraph (c) of Section 1.4. Thus, your request is denied pursuant to the first exemption of the FOIA which provides that the FOIA does not apply to matters that are specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign relations and are, in fact properly classified pursuant to such Executive Order.

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. The third exemption of the FOIA provides for the withholding of information specifically protected from disclosure by statute. Thus, your request is also denied because the fact of the existence or non-existence of the information is exempted from disclosure pursuant to the third exemption. The specific statutes applicable in this case are Title 18 U.S. Code 798; Title 50 U.S. Code 3024(i); and Section 6, Public Law 86-36 (50 U.S. Code 3605).

Sincerely,

A handwritten signature in black ink, appearing to read 'RM', is written over a horizontal line.

RONALD MAPP
Chief, FOIA/PA Office
NSA Initial Denial Authority

EXHIBIT D

THE TRANSPARENCY PROJECT

P.O. Box 20753
Brooklyn, New York 11202
(979) 985-5289

February 11, 2021

NSA/CSS FOIA Appeal Authority
National Security Agency
9800 Savage Road STE 6932
Ft. George G. Meade, MD 20755-6932

Via facsimile
443-479-3612

Re: Freedom of Information Act Request 109745

To Whom It May Concern:

I write to appeal the NSA's undated response (attached) to my FOIA request on behalf of The Transparency Project. Section 1.7 of Executive Order 13526 expressly prohibits the use of classification for purposes of concealing government misconduct or illegal activity. If government entities lied to Congress about the persons responsible for transferring emails from the Democratic National Committee to Wikileaks in 2016, *e.g.*, by shifting blame to Russian hackers rather than DNC employee Seth Rich, then classification of that information would be improper under EO 13526. Likewise, a *Glomar* response would be improper.

With respect to the matters in Request No. 3, the NSA would be fully expected to intercept communications between the Rich brothers and any foreign entities such as Wikileaks, therefore disclosure of the contents of those communications would not reveal anything about collection methods that is not already known.

Sincerely,



Ty Clevenger
Executive Director



NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 109745

TY CLEVENGER
THE TRANSPARENCY PROJECT
PO BOX 20753
BROOKLYN NY 11202-0753

Dear Ty Clevenger:

This responds to your Freedom of Information Act (FOIA) request of 12 June 2020, which was received by this office on 15 June 2020, for:

1. "I request the opportunity to view all metadata, communications (internal or external), records, documents, reports or other evidence regarding whether the National Security Agency (NSA), the Central Intelligence Agency (CIA), any "Five Eyes" allies, and/or affiliates, agents, employees or contractors of those agencies or any other government entity played a role in inserting Russian 'fingerprints' (e.g., 'COZY BEAR' or 'FANCYBEAR') into data from the 2016 Data Breach. In other words, the NSA should produce all evidence indicating whether any U.S. Government or 'Five Eyes' entities, affiliates, agents, employees or contractors inserted or fabricated evidence to make it appear that Russians or other third parties were responsible for the 2016 Data Breach. This includes, for example, any and all evidence that U.S. Government or 'Five Eyes' entity, affiliate, agent, employee, or contractor created or operated the 'Guccifer 2.0' or 'DCLeaks' profiles or any other online profile used to promote or distribute data from the 2016 Data Breach."
2. "I request the opportunity to view all tangible evidence reflecting the person, persons, or entities involved in 2016 Data Breach. This request includes, but is not limited to, evidence indicating whether the breach was the result of (1) outside forces (e.g., Russian agents, Pakistani agents, etc.) who hacked the servers from a remote location or (2) an individual or individuals who were present at or inside DNC facilities and copied the data onto a storage device. If, for example, NSA intercepted or obtained any communications between Seth Rich and Julian Assange or Wikileaks (e.g., from the United Kingdom's Government Communications Headquarters, or any other person or entity), then those communications should be produced. If the NSA has any evidence whatsoever that the DNC servers were hacked externally or that DNC data was leaked from an internal source, that evidence should be produced."
3. "I request the opportunity to view all communications exchanged (either directly or indirectly) between Seth Conrad Rich ('Seth Rich') and/or Aaron

FOIA Case: 109745

Nathan Rich ('Aaron Rich') and the following: Julian Assange, Wikileaks, and/or any agents or representatives of Wikileaks."

Your letter has been assigned Case Number 109745. Please refer to this case number when contacting us about your request. There are no assessable fees for this request; therefore, we did not address your fee category. Your request has been processed under the provisions of the FOIA.

NSA collects and provides intelligence derived from foreign communications to policymakers, military commanders, and law enforcement officials. We do this to help these individuals protect the security of the United States, its allies, and their citizens from threats such as terrorism, weapons of mass destruction, foreign espionage, international organized crime, and other hostile activities. What we are authorized to do, and how we do it, is described in Executive Order 12333. Information about how NSA conducts signals intelligence activities is available on the websites of NSA (www.nsa.gov) and the Office of the Director of National Intelligence (www.dni.gov).

We have determined that the fact of the existence or non-existence of the materials you request is a currently and properly classified matter in accordance with Executive Order 13526, as set forth in Subparagraph (c) of Section 1.4. Thus, your request is denied pursuant to the first exemption of the FOIA which provides that the FOIA does not apply to matters that are specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign relations and are, in fact properly classified pursuant to such Executive Order.

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. The third exemption of the FOIA provides for the withholding of information specifically protected from disclosure by statute. Thus, your request is also denied because the fact of the existence or non-existence of the information is exempted from disclosure pursuant to the third exemption. The specific statutes applicable in this case are Title 18 U.S. Code 798; Title 50 U.S. Code 3024(i); and Section 6, Public Law 86-36 (50 U.S. Code 3605).

Sincerely,

A handwritten signature in black ink, appearing to be 'RM' followed by a stylized flourish.

RONALD MAPP
Chief, FOIA/PA Office
NSA Initial Denial Authority

EXHIBIT E

Doc ID: 6716924

MIAMI RUBIO, NORTH CAROLINA, CHAIRMAN
MARK R. WARNER, VIRGINIA, VICE CHAIRMAN

JAMES E. RISCH, IDAHO	DIANNE FEINSTEIN, CALIFORNIA
MARCO RUBIO, FLORIDA	RON WYDEN, OREGON
SUSAN M. COLLINS, MAINE	MARTIN HEINRICH, NEW MEXICO
ROY BLUNT, MISSOURI	ANGUS S. KING, JR., MAINE
JAMES LANKFORD, OKLAHOMA	JOE MANCHIN, WEST VIRGINIA
TOM COTTON, ARKANSAS	KAMALA HARRIS, CALIFORNIA
JOHN CORNYN, TEXAS	

~~TOP SECRET//SI-G//NOFORN~~

United States Senate

SELECT COMMITTEE ON INTELLIGENCE

WASHINGTON, DC 20510-6475

MITCH McConnell, KENTUCKY, EX OFFICIO
CHARLES SCHUMER, NEW YORK, EX OFFICIO
JOHN M. CAIN, ARIZONA, EX OFFICIO
JACK REED, RHODE ISLAND, EX OFFICIO

CHRISTOPHER A. JOYNER, STAFF DIRECTOR
MICHAEL CASEY, MINORITY STAFF DIRECTOR
KEITSEY STROUD-BAILEY, CHIEF CLERK

April 4, 2018

SSCI# 2018-1104

Admiral Michael S. Rogers
Director
National Security Agency
Ft. Meade, MD 20755

(b) (1)
(b) (3) - P.L. 86-36

Dear Admiral Rogers:

(U) Thank you for the National Security Agency's (NSA) ongoing support of the Senate Select Committee on Intelligence's bipartisan inquiry [REDACTED]

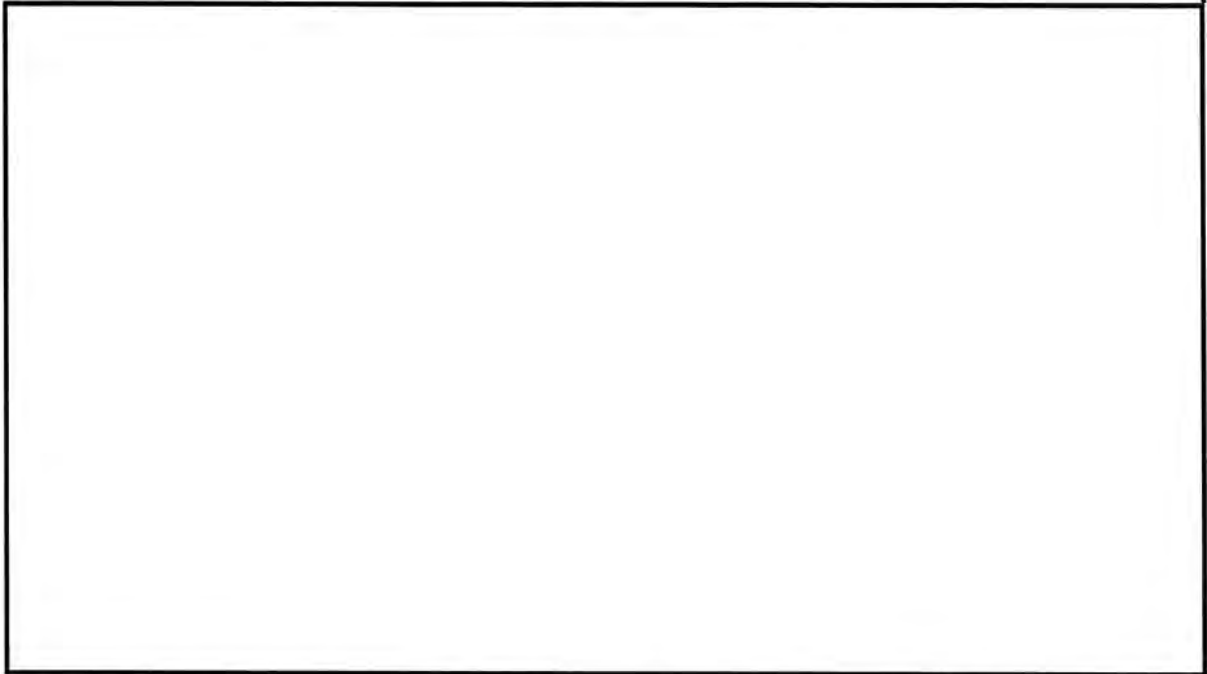
[REDACTED]

~~TOP SECRET//SI-G//NOFORN~~

Doc ID: 6716924

(b) (1)
(b) (3) - P.L. 86-36

~~TOP SECRET//SI-G//NOFORN~~



(U) In addition to retroactive production, prospective production should be made on a monthly basis, pursuant to the Committee's letter on May 23, 2017.

(U) Thank you for your attention to this matter. If you have any questions please contact [redacted] or [redacted] on the Committee staff.

Sincerely,

Richard Burr
Chairman

Mark R. Warner
Vice Chairman

(b) (6)

~~TOP SECRET//SI-G//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

NSA Response to QFRs from SSCI Worldwide Threats Hearing – Open Session 13 February 2018

[From Senator Rubio]

The National Security Strategy of the United States 2017 emphasizes, “The United States also remains committed to supporting and advancing religious freedom.”

1. *What kind of violations of and threats to religious freedom do you assess are threats to our national security? Which countries are the greatest offenders?*

Answer: (U) The National Security Strategy (NSS) recognizes that religious freedom is one of our country’s values and it is equally cherished by others throughout the world. Although the NSS does not state that a lack of religious freedom is a threat to national security, the denial of this right to individuals can be a destabilizing force within a society. Such destabilization can ultimately lead to conflict, and create U.S. national security concerns.

2. *What trends do you see regarding religious freedom violations, especially from governments justifying violations in the name of security and countering extremism?*

Answer: (U) I would refer the Committee to the State Department’s annual International Religious Freedom Report, detailing government policies violating religious belief and practices of groups, religious denominations and individuals, and U.S. policies to promote religious freedom around the world. The report is available at: <https://www.state.gov/j/drl/rls/irf/>.

3. *What is your assessment of the impact of these violations on our efforts to counter terrorists and violent extremists?*

Answer: (U) See answer to question #2 above.

The word “corruption” is mentioned 14 times in the National Security Strategy. Corruption enables authoritarian leaders to keep their cronies loyal and serves as a tool of statecraft by providing a backdoor to influence the politics of neighbors and rivals. This style of government by corruption, otherwise known as “kleptocracy,” is most clearly demonstrated by Russia, but appears to be spreading in parts of Europe, Eurasia, and Latin America.

4. *To what extent does globalized kleptocracy pose a threat to the national security of the United States and what can be done to combat it?*

Answer: (U) As the NSS notes, “[t]errorists and criminals thrive where governments are weak, corruption is rampant, and faith in government institutions is low.”

Classified By:

Derived From: NSA/CSSM 1-52

Dated: 20130930

Declassify On: 20430401

(b) (3) - P.L. 86-36

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

Terrorism and trans-national crime are ongoing threats to the national security of the United States; the forces that feed these threats are also national security concerns. For its part, NSA works to produce foreign intelligence in response to national security officials' requests for foreign intelligence regarding these topics.

5. *What is your evaluation of the extent to which Russia can be seen as a viable counterterrorism partner to the United States?*

Answer: (U) Effectively countering global terrorism often requires the help of other nations, and the United States government has a history of working with foreign partners to combat terrorism. Russia, like many other nations, could be a valuable partner in combating terrorism. That evaluation would be highly fact-dependent and, ultimately, a decision that NSA would inform, but would not make.

[From Senator Wyden]

In November 2017, I wrote to White House Cybersecurity Coordinator Rob Joyce, asking him to take steps to protect federal workers and their computers from malware delivered via advertising networks. As I noted in that letter, several federal agencies have already deployed network-based advertising blocking technology.

6. *In the NSA's view, how serious is the threat posed to federal computers by malware delivered via commercial advertising networks?*

Answer: (U) Commercial advertising networks provide a lucrative avenue for attackers to deliver exploits because it enables them to leverage sites their intended targets visit on a regular basis and are more likely to trust. However, this is just one of many methods that can be used to deliver malware and no single method should be a point of focus to the exclusion of others.

7. *Does the NSA recommend government agencies block advertising networks from delivering executable code to computer and mobile devices of federal workers?*

Answer: (U) NSA strongly advocates for a defense-in-depth approach to security. As such, all reasonable steps to protect federal networks and information should be taken, which may include blocking threatening Internet content. However, no single approach is foolproof. NSA encourages all federal departments and agencies to leverage best practices, patch management, and to use up-to date endpoint, network-security products, and updated browsers, to reduce the risk of exploitation by malicious advertisers.

8. *Do you believe there is a legitimate government interest in protecting the personal accounts and devices of government officials?*

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

Answer: (U) The personal devices and accounts of a wide range of government officials remain natural targets for exploitation. We must raise awareness so all government employees use proper cyber hygiene. Ultimately, the security of personal devices and accounts remains an individual's responsibility.

9. *If yes, what steps, if any, have your agencies taken to improve the security of your employees' personal accounts and devices?*

Answer: (U) As stated in response to question 8, ultimately, the security of personal devices and accounts remains an individual's responsibility. However, NSA can and does contribute to wider governmental efforts to counter malicious cyber activity. For example, NSA regularly collaborates with the Department of Homeland Security (DHS) and other Executive Branch agencies regarding cyber security threat, vulnerabilities, and mitigations. For public awareness, NSA publishes unclassified guidance on how users can secure their communications devices, computing equipment, and networks.

10. *What resources do you need in order to ensure that these personal accounts and devices are not a vulnerable target for foreign intelligence services?*

Answer: (U) As stated in response to question 8, ultimately, the security of personal devices and accounts remains an individual's responsibility.

[From Senator Cotton]

In 2017, The Director of the Central Intelligence Agency referred to Wikileaks as a "non-state hostile intelligence service" that often aids U.S. adversaries like Russia and China. At my request, Chairman Burr and Vice-Chairman Warner included language to that effect in the FY17 Intelligence Authorization Act.

11. *Do you agree with Director Pompeo and this Committee that Wikileaks is a non-state hostile intelligence service that often aids U.S. adversaries like Russia?*

(b) (5)

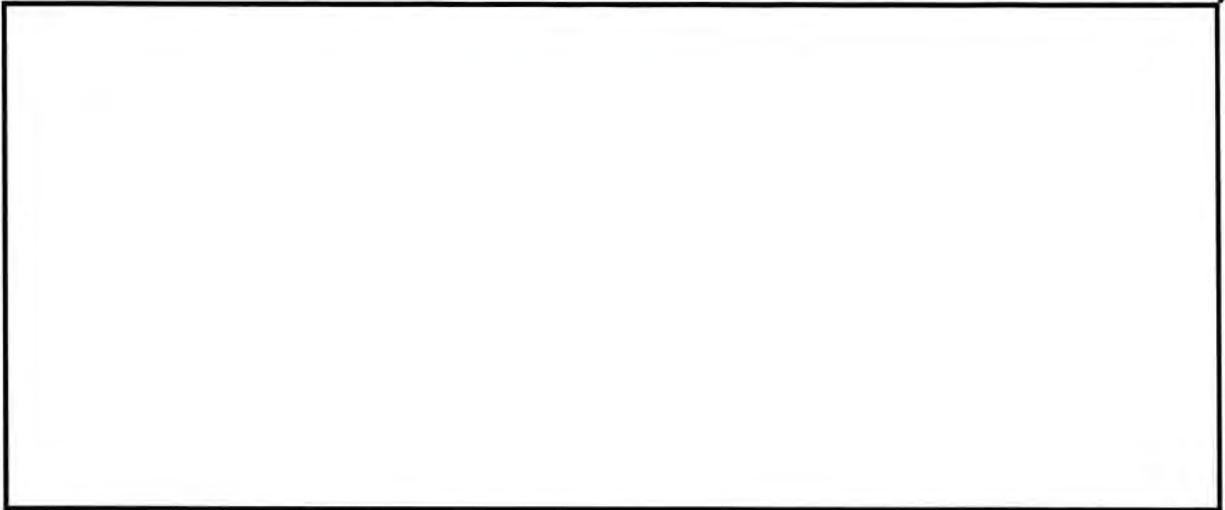
[From Senator Harris]

Under the Administration's new Vulnerabilities Equities Process (VEP) charter, the NSA serves as the Executive Secretariat and is responsible for producing an annual report to Congress – the first report will come out this year.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

(b) (5)



14. Please confirm that DoD receives one vote.

Answer: (U) Per the UNCLASSIFIED VEP Charter dated 15 November 2017, the Department of Defense (DoD) is one of the 18 participating members of the VEP Equities Review Board (ERB). Several of the departments and agencies on the ERB are represented by multiple component entities, including DoD, DHS, and DoJ. DoD, at the departmental level, is typically represented by the Office of the Secretary of Defense, but DoD components with unique technical and operational knowledge also participate and may vote separately in the ERB, including NSA, USCYBERCOM, and the DoD Cyber Crime Center (DC3). It is important to note, however, that if there is disagreement about an ERB decision based on a non-unanimous vote, that issue can be elevated for higher-level decision through the process described in National Security Presidential Memorandum (NSPM)-4.

15. Please confirm whether that one vote is allocated to the NSA.

Answer: (U) See answer to question #14 above.

~~TOP SECRET//SI//ORCON/NOFORN~~

Doc ID: 6716926

~~TOP SECRET//SI//NOFORN~~

NSA Response to QFRs from SSCI Worldwide Threats Hearing – Closed Session 13 February 2018

(b) (1)
(b) (3) – P.L. 86-36

[From Senator Cotton]

1.

2.

3.

Answer: (TS//SI//NF)

(b) (3) – P.L. 86-36

Classified By: [REDACTED]

Derived From: NSA/CSSM 1-52

Dated: 20130930

Declassify On: 20430401

~~TOP SECRET//SI//NOFORN~~

Approved for Release by NSA on 01-28-2021, FOIA Litigation Case # 105508

TTP NSA 000007

Doc ID: 6716927

BURR, NORTH CAROLINA, CHAIRMAN
MARK R. WARNER, VIRGINIA, VICE CHAIRMAN

JAMES E. RISCH, IDAHO
MARCO RUBIO, FLORIDA
SUSAN M. COLLINS, MAINE
ROY BLUNT, MISSOURI
JAMES LANKFORD, OKLAHOMA
TOM COTTON, ARKANSAS
JOHN CORNYN, TEXAS

DIANNE FEINSTEIN, CALIFORNIA
RON WYDEN, OREGON
MARTIN HEINRICH, NEW MEXICO
ANGUS S. KING, JR., MAINE
JOE MANCHIN, WEST VIRGINIA
KAMALA HARRIS, CALIFORNIA

MITCH MCCONNELL, KENTUCKY, EX OFFICIO
CHARLES SCHUMER, NEW YORK, EX OFFICIO
JOHN MCCAIN, ARIZONA, EX OFFICIO
JACK REED, RHODE ISLAND, EX OFFICIO

CHRISTOPHER A. JOYNER, STAFF DIRECTOR
MICHAEL CASLEY, MINORITY STAFF DIRECTOR
KEYSE STROUD BAILEY, CHIEF CLERK

United States Senate

SELECT COMMITTEE ON INTELLIGENCE
WASHINGTON, DC 20510-6475

March 22, 2018

Admiral Michael S. Rogers
Director
National Security Agency
Washington, D.C. 20701

SSCI# 2018-1088

Dear Admiral Rogers:

We appreciate your testimony at the Worldwide Threats Hearing on February 13, 2018. We are submitting the attached questions for the record and would appreciate a response by April 27, 2018.

If your staff has any questions, please contact [redacted] or [redacted]
[redacted] of the Committee staff at [redacted].

(b) (6)

Sincerely,



Richard Burr
Chairman



Mark R. Warner
Vice Chairman

**Questions for the Record
Senate Select Committee on Intelligence
Worldwide Threats Hearing – Open Session
February 13, 2018**

**Questions for the Record for Admiral Michael S. Rogers, Director of the
National Security Agency**

[From Senator Rubio]

The National Security Strategy of the United States 2017 emphasizes, “The United States also remains committed to supporting and advancing religious freedom.”

- 1. What kind of violations of and threats to religious freedom do you assess are threats to our national security? Which countries are the greatest offenders?**
- 2. What trends do you see regarding religious freedom violations, especially from governments justifying violations in the name of security or countering extremism?**
- 3. What is your assessment of the impact of these violations on our efforts to counter terrorists and violent extremists?**

The word “corruption” is mentioned 14 times in the National Security Strategy. Corruption enables authoritarian leaders to keep their cronies loyal and serves as a tool of statecraft by providing a backdoor to influence the politics of neighbors and rivals. This style of government by corruption, otherwise known as “kleptocracy,” is most clearly demonstrated by Russia, but appears to be spreading in parts of Europe, Eurasia, and Latin America.¹

- 4. To what extent does globalized kleptocracy pose a threat to the national security of the United States and what can be done to combat it?**

¹ In your response, please describe how the interests of the United States and Russia converge and diverge in confronting the Islamic State and related groups; confronting extremist groups in Afghanistan; and countering growing extremism in areas such as Central Asia and the Balkans.

5. What is your evaluation of the extent to which Russia can be seen as a viable counterterrorism partner to the United States?

[From Senator Wyden]

In November 2017, I wrote to White House Cybersecurity Coordinator Rob Joyce, asking him to take steps to protect federal workers and their computers from malware delivered via advertising networks. As I noted in that letter, several federal agencies have already deployed network-based advertising blocking technology.

6. In the NSA's view, how serious is the threat posed to federal computers by malware delivered via commercial advertising networks?

7. Does the NSA recommend that government agencies block advertising networks from delivering executable code to the computers and mobile devices of federal workers?

Recent news reports indicate that the same Russian hackers who infiltrated the Democratic National Committee in 2016 and the German Bundestag in 2014 repeatedly targeted senior U.S. government officials, defense contractors, and scientists through their personal email accounts. (AP, "'Fancy Bear' hackers took aim at US defense contractors," February 7, 2018.)

8. Do you believe there is a legitimate government interest in protecting the personal accounts and devices of government officials?

9. If yes, what steps, if any, have your agencies taken to improve the security of your employees' personal accounts and devices?

10. What resources do you need in order to ensure that these personal accounts and devices are not a vulnerable target for foreign intelligence services?

[From Senator Cotton]

In 2017, the Director of the Central Intelligence Agency referred to WikiLeaks as a "non-state hostile intelligence service" that often aids U.S. adversaries like Russia and China. At my request, Chairman Burr and Vice-Chairman Warner included language to that effect in the FY17 Intelligence Authorization Act.

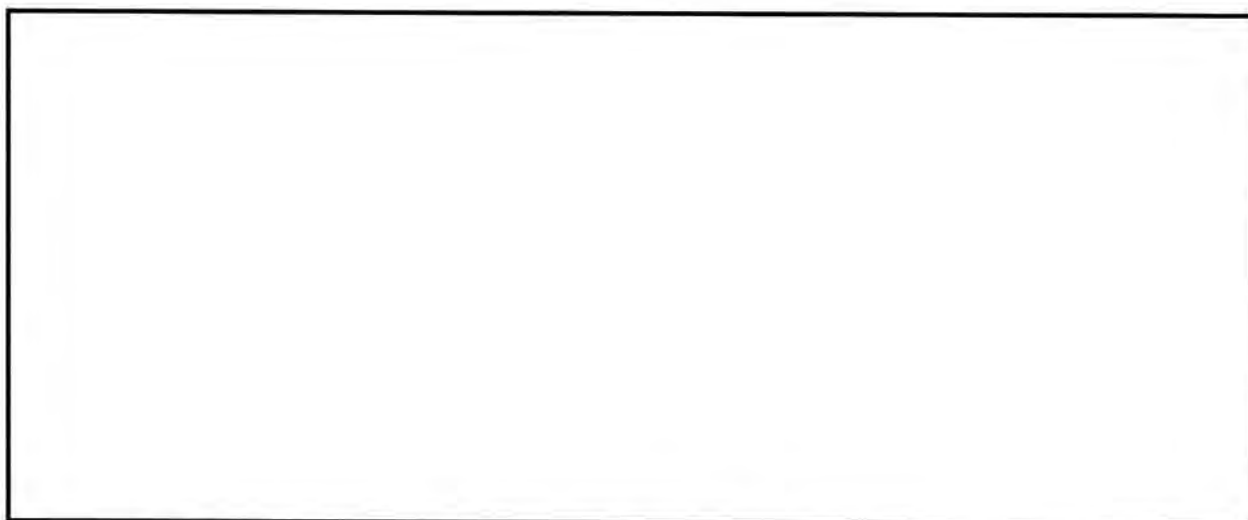
11. Do you agree with Director Pompeo and this Committee that WikiLeaks is a non-state hostile intelligence service that often aids U.S. adversaries like Russia?

[From Senator Harris]

Under the Administration's new Vulnerabilities Equities Process (VEP) charter, the NSA serves as the Executive Secretariat and is responsible for producing an annual report to Congress – the first report will come out this year.

(b) (5)

⋮



14. Please confirm that DOD receives one vote.

15. Please confirm whether that one vote is allocated to the NSA.

Doc ID: 6716928

RICHARD BURR, NORTH CAROLINA, CHAIRMAN
 MARK R. WARNER, VIRGINIA, VICE CHAIRMAN

JAMES E. RISCH, IDAHO
 MARCO RUBIO, FLORIDA
 SUSAN M. COLLINS, MAINE
 ROY BLUNT, MISSOURI
 JAMES TANKFORD, OKLAHOMA
 TOM COTTON, ARKANSAS
 JOHN CORNYN, TEXAS

DIANNE FEINSTEIN, CALIFORNIA
 RON WYDEN, OREGON
 MARTIN HEINRICH, NEW MEXICO
 ANGUS S. KING, J., MAINE
 JOE MANCHIN, WEST VIRGINIA
 KAMALA HARRIS, CALIFORNIA

~~TOP SECRET//SI//NOFORN~~

United States Senate

SELECT COMMITTEE ON INTELLIGENCE

WASHINGTON, DC 20510-6475

MITCH MCCONNELL, KENTUCKY, EX OFFICIO
 CHARLES SCHUMER, NEW YORK, EX OFFICIO
 JOHN MCCAIN, ARIZONA, EX OFFICIO
 JACK REED, RHODE ISLAND, EX OFFICIO

CHRISTOPHER A. JOYNER, STAFF DIRECTOR
 MICHAEL CASEY, MINORITY STAFF DIRECTOR
 KELSEY STROUD BAILEY, CHIEF CLERK

March 22, 2018

Admiral Michael S. Rogers
 Director
 National Security Agency
 Washington, D.C. 20701

SSCI# 2018-1087

Dear Admiral Rogers:

We appreciate your testimony at the Worldwide Threats Hearing on February 13, 2018. We are submitting the attached classified questions for the record and would appreciate a response by April 27, 2018.

If your staff has any questions, please contact [redacted] or [redacted]
 [redacted] of the Committee staff at [redacted]

Sincerely,

(b) (6)



Richard Burr
 Chairman



Mark R. Warner
 Vice Chairman

Approved for Release by NSA on 01-28-2021, FOIA Litigation Case # 105508

~~TOP SECRET//SI//NOFORN~~

TTP NSA 000012

2018-03030

Doc ID: 6716928

~~TOP SECRET//SI//NOFORN~~

Questions for the Record
Senate Select Committee on Intelligence
Worldwide Threat Hearing – Closed Session
February 13, 2018

**Questions for the Record for Admiral Michael S. Rogers, Director of the
National Security Agency**

(b) (1)
(b) (3) - P.L. 86-36

[From Senator Cotton]

1.

[Redacted]

2.

[Redacted]

3.

[Redacted]

~~TOP SECRET//SI//NOFORN~~

TTP NSA 000013

EXHIBIT F



NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 105508B
10 February 2022

TY CLEVINGER
THE TRANSPARENCY PROJECT
PO BOX 20753
BROOKLYN NY 11202-0753

Dear Ty Clevenger:

This updates our response to your Freedom of Information Act (FOIA) request of 29 October 2018 for the twelve items listed below:

1. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Seth Conrad Rich.
2. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Julian Assange.
3. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Wikileaks.
4. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Kim Dotcom.
5. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Aaron Rich.
6. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Shawn Lucas.
7. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Kelsey Mulka.

FOIA Case: 105508B

8. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Imran Iwan.

9. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Abid Awan.

10. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Jamal Awan.

11. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Hina Alvi.

12. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Rao Abbas.

Since our 2 February 2021 response to you, we determined that some redactions can be lifted in two of the documents. We also determined that other information was properly redacted, but the incorrect FOIA Exemption was cited. We have reviewed the two documents (8 pages) in their entirety and are providing updated versions.

Some of the withheld information has been found to be currently and properly classified in accordance with Executive Order 13526. The information meets the criteria for classification as set forth in Subparagraph (c) of Section 1.4 and remains classified TOP SECRET. The information is classified because its disclosure could reasonably be expected to cause exceptionally grave damage to the national security. Because the information is currently and properly classified, it is exempt from disclosure pursuant to the first exemption of the FOIA (5 U.S.C. Section 552(b)(1)).

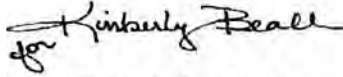
In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. We have determined that such information exists in these documents. Accordingly, those portions are exempt from disclosure pursuant to the third exemption of the FOIA, which provides for the withholding of information specifically protected from disclosure by statute. The specific statute applicable in this case is Section 6, Public Law 86-36 (50 U.S. Code 3605).

Lastly, personal information regarding individuals has been withheld from the enclosures in accordance with 5 U.S.C. 552 (b)(6). This exemption protects from disclosure information that would constitute a clearly unwarranted invasion of personal privacy. In balancing the public interest for the information you request against the privacy interests involved, we have

FOIA Case: 105508B

determined that the privacy interests sufficiently satisfy the requirements for the application of the (b)(6) exemption.

Sincerely,

A handwritten signature in black ink, appearing to read "Paula A. Gill". The signature is fluid and cursive, with a small "for" written below the main name.

PAULA A. GILL
Chief, FOIA/PA Division
NSA Initial Denial Authority

Encls:
a/s

~~TOP SECRET//SI//ORCON/NOFORN~~

NSA Response to QFRs from SSCI Worldwide Threats Hearing – Open Session 13 February 2018

[From Senator Rubio]

The National Security Strategy of the United States 2017 emphasizes, “The United States also remains committed to supporting and advancing religious freedom.”

1. *What kind of violations of and threats to religious freedom do you assess are threats to our national security? Which countries are the greatest offenders?*

Answer: (U) The National Security Strategy (NSS) recognizes that religious freedom is one of our country’s values and it is equally cherished by others throughout the world. Although the NSS does not state that a lack of religious freedom is a threat to national security, the denial of this right to individuals can be a destabilizing force within a society. Such destabilization can ultimately lead to conflict, and create U.S. national security concerns.

2. *What trends do you see regarding religious freedom violations, especially from governments justifying violations in the name of security and countering extremism?*

Answer: (U) I would refer the Committee to the State Department’s annual International Religious Freedom Report, detailing government policies violating religious belief and practices of groups, religious denominations and individuals, and U.S. policies to promote religious freedom around the world. The report is available at: <https://www.state.gov/j/drl/rls/irf/>.

3. *What is your assessment of the impact of these violations on our efforts to counter terrorists and violent extremists?*

Answer: (U) See answer to question #2 above.

The word “corruption” is mentioned 14 times in the National Security Strategy. Corruption enables authoritarian leaders to keep their cronies loyal and serves as a tool of statecraft by providing a backdoor to influence the politics of neighbors and rivals. This style of government by corruption, otherwise known as “kleptocracy,” is most clearly demonstrated by Russia, but appears to be spreading in parts of Europe, Eurasia, and Latin America.

4. *To what extent does globalized kleptocracy pose a threat to the national security of the United States and what can be done to combat it?*

Answer: (U) As the NSS notes, “[t]errorists and criminals thrive where governments are weak, corruption is rampant, and faith in government institutions is low.”

Classified By:

Derived From: NSA/CSSM 1-52

Dated: 20130930

Declassify On: 20430401

(b) (3) - P.L. 86-36

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

Terrorism and trans-national crime are ongoing threats to the national security of the United States; the forces that feed these threats are also national security concerns. For its part, NSA works to produce foreign intelligence in response to national security officials' requests for foreign intelligence regarding these topics.

5. *What is your evaluation of the extent to which Russia can be seen as a viable counterterrorism partner to the United States?*

Answer: (U) Effectively countering global terrorism often requires the help of other nations, and the United States government has a history of working with foreign partners to combat terrorism. Russia, like many other nations, could be a valuable partner in combating terrorism. That evaluation would be highly fact-dependent and, ultimately, a decision that NSA would inform, but would not make.

[From Senator Wyden]

In November 2017, I wrote to White House Cybersecurity Coordinator Rob Joyce, asking him to take steps to protect federal workers and their computers from malware delivered via advertising networks. As I noted in that letter, several federal agencies have already deployed network-based advertising blocking technology.

6. *In the NSA's view, how serious is the threat posed to federal computers by malware delivered via commercial advertising networks?*

Answer: (U) Commercial advertising networks provide a lucrative avenue for attackers to deliver exploits because it enables them to leverage sites their intended targets visit on a regular basis and are more likely to trust. However, this is just one of many methods that can be used to deliver malware and no single method should be a point of focus to the exclusion of others.

7. *Does the NSA recommend government agencies block advertising networks from delivering executable code to computer and mobile devices of federal workers?*

Answer: (U) NSA strongly advocates for a defense-in-depth approach to security. As such, all reasonable steps to protect federal networks and information should be taken, which may include blocking threatening Internet content. However, no single approach is foolproof. NSA encourages all federal departments and agencies to leverage best practices, patch management, and to use up-to date endpoint, network-security products, and updated browsers, to reduce the risk of exploitation by malicious advertisers.

8. *Do you believe there is a legitimate government interest in protecting the personal accounts and devices of government officials?*

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

Answer: (U) The personal devices and accounts of a wide range of government officials remain natural targets for exploitation. We must raise awareness so all government employees use proper cyber hygiene. Ultimately, the security of personal devices and accounts remains an individual's responsibility.

9. *If yes, what steps, if any, have your agencies taken to improve the security of your employees' personal accounts and devices?*

Answer: (U) As stated in response to question 8, ultimately, the security of personal devices and accounts remains an individual's responsibility. However, NSA can and does contribute to wider governmental efforts to counter malicious cyber activity. For example, NSA regularly collaborates with the Department of Homeland Security (DHS) and other Executive Branch agencies regarding cyber security threat, vulnerabilities, and mitigations. For public awareness, NSA publishes unclassified guidance on how users can secure their communications devices, computing equipment, and networks.

10. *What resources do you need in order to ensure that these personal accounts and devices are not a vulnerable target for foreign intelligence services?*

Answer: (U) As stated in response to question 8, ultimately, the security of personal devices and accounts remains an individual's responsibility.

[From Senator Cotton]

In 2017, The Director of the Central Intelligence Agency referred to Wikileaks as a "non-state hostile intelligence service" that often aids U.S. adversaries like Russia and China. At my request, Chairman Burr and Vice-Chairman Warner included language to that effect in the FY17 Intelligence Authorization Act.

11. *Do you agree with Director Pompeo and this Committee that Wikileaks is a non-state hostile intelligence service that often aids U.S. adversaries like Russia?*

Answer: ~~(TS//SI//OC/NF)~~ [REDACTED]

(b) (1)
(b) (3) - P.L. 86-36

[From Senator Harris]

Under the Administration's new Vulnerabilities Equities Process (VEP) charter, the NSA serves as the Executive Secretariat and is responsible for producing an annual report to Congress – the first report will come out this year.

12. *Will you commit that, to the greatest extent possible while protecting sources and methods, the NSA will include in its unclassified report how the VEP handled each serious vulnerability that it considered?*

~~TOP SECRET//SI//ORCON//NOFORN~~

Doc ID: 6755074

~~TOP SECRET//SI//ORCON//NOFORN~~

(b) (3) - P.L. 86-36

Answer: (U//~~FOUO~~)

13. *Additionally, will you commit that the annual report will include, as a classified annex, a more detailed list of the vulnerabilities that the VEP considered and the decision that was made on each?*

Answer: (U) See answer to question #12 above.

14. *Please confirm that DoD receives one vote.*

Answer: (U) Per the UNCLASSIFIED VEP Charter dated 15 November 2017, the Department of Defense (DoD) is one of the 18 participating members of the VEP Equities Review Board (ERB). Several of the departments and agencies on the ERB are represented by multiple component entities, including DoD, DHS, and DoJ. DoD, at the departmental level, is typically represented by the Office of the Secretary of Defense, but DoD components with unique technical and operational knowledge also participate and may vote separately in the ERB, including NSA, USCYBERCOM, and the DoD Cyber Crime Center (DC3). It is important to note, however, that if there is disagreement about an ERB decision based on a non-unanimous vote, that issue can be elevated for higher-level decision through the process described in National Security Presidential Memorandum (NSPM)-4.

15. *Please confirm whether that one vote is allocated to the NSA.*

Answer: (U) See answer to question #14 above.

~~TOP SECRET//SI//ORCON//NOFORN~~

Doc ID: 6755148

MARK R. BURR, NORTH CAROLINA, CHAIRMAN
MARK R. WARNER, VIRGINIA, VICE CHAIRMAN
JAMES E. RISCH, IDAHO
MARCO RUBIO, FLORIDA
SUSAN M. COLLINS, MAINE
ROY BLUNT, MISSOURI
JAMES LANKFORD, OKLAHOMA
TOM COTTON, ARKANSAS
JOHN CORNYN, TEXAS
DIANNE FEINSTEIN, CALIFORNIA
RON WYDEN, OREGON
MARTIN HEINRICH, NEW MEXICO
ANGUS S. KING, JR., MAINE
JOE MANCHIN, WEST VIRGINIA
KAMALA HARRIS, CALIFORNIA

United States Senate

SELECT COMMITTEE ON INTELLIGENCE
WASHINGTON, DC 20510-6475

MITCH MCCONNELL, KENTUCKY, EX OFFICIO
CHARLES SCHUMER, NEW YORK, EX OFFICIO
JOHN MCCAIN, ARIZONA, EX OFFICIO
JACK REED, RHODE ISLAND, EX OFFICIO

CHRISTOPHER A. JOYNER, STAFF DIRECTOR
MICHAEL CASEY, MINORITY STAFF DIRECTOR
KELSEY STROUD BAILEY, CHIEF CLERK

March 22, 2018

Admiral Michael S. Rogers
Director
National Security Agency
Washington, D.C. 20701

SSCI# 2018-4088

Dear Admiral Rogers:

We appreciate your testimony at the Worldwide Threats Hearing on February 13, 2018. We are submitting the attached questions for the record and would appreciate a response by April 27, 2018.

If your staff has any questions, please contact [redacted] or [redacted]
[redacted] of the Committee staff at [redacted]

(b) (6)

Sincerely,



Richard Burr
Chairman



Mark R. Warner
Vice Chairman

Questions for the Record
Senate Select Committee on Intelligence
Worldwide Threats Hearing – Open Session
February 13, 2018

Questions for the Record for Admiral Michael S. Rogers, Director of the National Security Agency

[From Senator Rubio]

The National Security Strategy of the United States 2017 emphasizes, “The United States also remains committed to supporting and advancing religious freedom.”

- 1. What kind of violations of and threats to religious freedom do you assess are threats to our national security? Which countries are the greatest offenders?**
- 2. What trends do you see regarding religious freedom violations, especially from governments justifying violations in the name of security or countering extremism?**
- 3. What is your assessment of the impact of these violations on our efforts to counter terrorists and violent extremists?**

The word “corruption” is mentioned 14 times in the National Security Strategy. Corruption enables authoritarian leaders to keep their cronies loyal and serves as a tool of statecraft by providing a backdoor to influence the politics of neighbors and rivals. This style of government by corruption, otherwise known as “kleptocracy,” is most clearly demonstrated by Russia, but appears to be spreading in parts of Europe, Eurasia, and Latin America.¹

- 4. To what extent does globalized kleptocracy pose a threat to the national security of the United States and what can be done to combat it?**

¹ In your response, please describe how the interests of the United States and Russia converge and diverge in confronting the Islamic State and related groups; confronting extremist groups in Afghanistan; and countering growing extremism in areas such as Central Asia and the Balkans.

5. What is your evaluation of the extent to which Russia can be seen as a viable counterterrorism partner to the United States?

[From Senator Wyden]

In November 2017, I wrote to White House Cybersecurity Coordinator Rob Joyce, asking him to take steps to protect federal workers and their computers from malware delivered via advertising networks. As I noted in that letter, several federal agencies have already deployed network-based advertising blocking technology.

- 6. In the NSA's view, how serious is the threat posed to federal computers by malware delivered via commercial advertising networks?**
- 7. Does the NSA recommend that government agencies block advertising networks from delivering executable code to the computers and mobile devices of federal workers?**

Recent news reports indicate that the same Russian hackers who infiltrated the Democratic National Committee in 2016 and the German Bundestag in 2014 repeatedly targeted senior U.S. government officials, defense contractors, and scientists through their personal email accounts. (AP, "'Fancy Bear' hackers took aim at US defense contractors," February 7, 2018.)

- 8. Do you believe there is a legitimate government interest in protecting the personal accounts and devices of government officials?**
- 9. If yes, what steps, if any, have your agencies taken to improve the security of your employees' personal accounts and devices?**
- 10. What resources do you need in order to ensure that these personal accounts and devices are not a vulnerable target for foreign intelligence services?**

[From Senator Cotton]

In 2017, the Director of the Central Intelligence Agency referred to WikiLeaks as a "non-state hostile intelligence service" that often aids U.S. adversaries like Russia and China. At my request, Chairman Burr and Vice-Chairman Warner included language to that effect in the FY17 Intelligence Authorization Act.

11. Do you agree with Director Pompeo and this Committee that WikiLeaks is a non-state hostile intelligence service that often aids U.S. adversaries like Russia?

[From Senator Harris]

Under the Administration's new Vulnerabilities Equities Process (VEP) charter, the NSA serves as the Executive Secretariat and is responsible for producing an annual report to Congress – the first report will come out this year.

12. Will you commit that, to the greatest extent possible while protecting sources and methods, the NSA will include in its unclassified report how the VEP handled each serious vulnerability that it considered?

13. Additionally, will you commit that the annual report will include, as a classified annex, a more detailed list of the vulnerabilities that the VEP considered and the decision that was made on each?

The Administration's new VEP charter is somewhat ambiguous about how voting in the VEP works, and whether intelligence and law enforcement agencies get multiple votes.

14. Please confirm that DOD receives one vote.

15. Please confirm whether that one vote is allocated to the NSA.

The Transparency Project v. U.S. Department of Justice, et. al

Civil Action No. 4:20-CV-467
U.S. District Court
Easter District of Texas
Sherman Division

Vaughn Index

This index contains a description of the records withheld in full or in part by the NSA. The disposition of the document(s) is noted with a “PR” for Partial Release and a “DIF” for Denied in Full. The documents described below were located in response to the Plaintiff’s October 29, 2018 request.

Date of Document	Description	Disposition	Exemption(s)	Pages
March 22, 2018	Letter from the Senate Select Committee on Intelligence (“SSCI”) to Director of the National Security Agency (“DIRNSA”) with Questions for the Record (“QFRs”) from Senator Cotton	PR	1 – classified information; 3 – P.L. 86-36 6 – privacy interest	2 total: Letter – 1 page; QFRs – 1 page
March 22, 2018	Letter from SSCI to DIRNSA with QFRs from Senators Rubio, Wyden, Cotton, and Harris	PR	6 – privacy interest	4 total: Letter – 1 page; QFRs – 3 pages
Not dated	NSA’s responses to Senator Cotton’s QFRs	PR	1 – classified information 3 – P.L. 86-36	1 total
Not dated	NSA’s responses to Senators Rubio, Wyden, Cotton, and Harris’s QFRs	PR	1 – classified information; 3 – P.L. 86-36	4 total
April 4, 2018	Letter from SSCI to DIRNSA	PR	1 – classified information; 3 – P.L. 86-36 6 – privacy interest	2 total
January 25, 2017	Correspondence with SSCI	DIF	1 – classified information 3 – P.L. 86-36 3 – 18 U.S.C. § 798 3 – 50 U.S.C. § 3024(i)(1)	2 total

January 25, 2017	Correspondence with Senate Committee on Appropriations, Subcommittee on Defense	DIF	1 – classified information 3 – P.L. 86-36 3 – 18 U.S.C. § 798 3 – 50 U.S.C. § 3024(i)(1)	2 total
January 25, 2017	Correspondence with House Permanent Select Committee on Intelligence (“HPSCI”)	DIF	1 – classified information 3 – P.L. 86-36 3 – 18 U.S.C. § 798 3 – 50 U.S.C. § 3024(i)(1)	2 total
January 25, 2017	Correspondence with House Committee on Appropriations, Subcommittee on Defense	DIF	1 – classified information 3 – P.L. 86-36 3 – 18 U.S.C. § 798 3 – 50 U.S.C. § 3024(i)(1)	2 total
March 2, 2017	Correspondence with SSCI; Senate Committee on Appropriations, Subcommittee on Defense; HPSCI; House Committee on Appropriations, Subcommittee on Defense	DIF	1 – classified information 3 – P.L. 86-36 3 – 18 U.S.C. § 798 3 – 50 U.S.C. § 3024(i)(1)	4 total: 1 page per correspondence
June 16, 2017	Correspondence with SSCI; Senate Committee on Appropriations, Subcommittee on Defense; HPSCI; House Committee on Appropriations, Subcommittee on Defense	DIF	1 – classified information 3 – P.L. 86-36 3 – 18 U.S.C. § 798 3 – 50 U.S.C. § 3024(i)(1)	4 total: 1 page per correspondence